ENUMERATION OF SOME TWO-GENERATOR GROUPS OF PRIME POWER ORDER

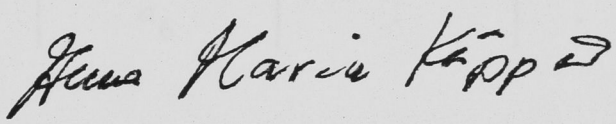
by

A.M. Küpper

A thesis submitted to the
Australian National University
for the degree of
Master of Science
December, 1979

STATEMENT

Except where otherwise stated, the work in this thesis is my own.



A.M. Küpper

CORRECTIONS

to

ENUMERATION OF SOME TWO-GENERATOR GROUPS OF PRIME POWER ORDER

by

A.M. Küpper

Page 75: Add to Family 2-22-14

Name	Name (James)	$[a_5, a_2]$	$[a_3, a_1]$	a_4^p	a_1^p
2-22-14-16	$\Phi_9(2211)b_r$	a_6	.	.	a_6^b

Page 77: Add to Family 2-22

Name	Name (James)	$[a_3, a_1]$	$[a_3, a_2]$	a_4^p	a_1^p
2-22-29	$\Phi_3(3111)e$	a_5	.	a_6	.
2-22-210	$\Phi_3(321)d$	a_5	.	a_6	a_5
2-22-211	$\Phi_3(3111)d$	.	a_5	a_6	.
2-22-212a	$\Phi_3(321)b_r$	.	a_5	a_6	a_5^a

21 December 1979

Additional corrections 5 March 1980

Page 60, line 4

Replace 'class c' by '(exponent-p-central) class c'

Page 69, line 3 should read:

Family relations: $[a_4, a_i] = a_3^p = e$, $i = 1, 2$.

Page 73, line 11 should read:

Family relations: $[a_4, a_2] = [a_5, a_1] = a_i^p = e$, $i = 4, 5$,

$$[a_5, a_2]^{-1} = [a_4, a_1]^{-\varepsilon} = a_3^p$$

Page 74, line 15 should read:

Family relations: $[a_i, a_1] = [a_i, a_2] = e$, $i = 3, 4$

Page 76, line 3, 4 should read:

Family relations: $a_3^p = [a_4, a_1] = [a_5, a_2]^{-a}$, $[a_5, a_1] = a_5^p = e$

The range of z is $(p - 3)/2 \leq z < p$.

Page 75, first table

Replace all 'a_5' in last column by '$a_5{}^a$'

Page 78, line 6

Replace 'Famil' by 'Family'

Page 78, line 8

Replace '$[a_5, a_1] = e$' by '$[a_5, a_2] = e$'

ACKNOWLEDGEMENTS

This thesis was produced with the help of many people. Dr H. Wolff of Christian Albrechts Universität Kiel, Germany first give me the confidence to continue my studies in mathematics; and the German Academic Exchange Service (DAAD) provided me with a one-year scholarship to come to Australia to do just that.

In Australia, my supervisor Dr M.F. Newman was always available for discussions. His constructive criticism and advice proved most helpful and he often saw a better way of handling the detailed calculations which go with a thesis of this type. Dr G. Havas and W. Alford also gave valuable assistance with computations.

Discussions with my fellow students were very fruitful. U. Kuhn and M. Schooneveldt read the whole draft and provided many discerning comments. Talks with L. Sterling and J. Ascione were very stimulating. In particular, J. Ascione provided a copy of her own thesis whose influence on this thesis is readily apparent.

I would also like to thank B. Geary for both her excellent typing and the benefit of her wide experience in transferring mathematical papers to print.

Finally, the ANU provided me with the opportunity and facilities for studying and, when my DAAD Scholarship ended, a Postgraduate Scholarship to continue the work.

ABSTRACT

This thesis gives a list of all 2-generator p-groups of order up to p^6, $p \geq 7$, using an algorithm described by M.F. Newman [1976]. The theoretical background of the algorithm is outlined in the first five chapters, and interesting calculations are discussed in Chapter 6. In the last chapter standard presentations for all 2-generator p-groups of order up to p^6, $p \geq 7$, are given. They are also represented graphically. Furthermore, the groups are identified with those in the list given by James [1969]. Our list agrees with his except for one discrepancy which is detailed in Chapter 6.

TABLE OF CONTENTS

NOTATION

$A \times B$	direct product of groups A and B
G/A	factor group of the group G by a normal subgroup A
$N_G(A)$	normalizer of the subgroup A in the group G
$Z(G)$	centre of the group G
$Z^p(G)$	p-centre of the group G
G'	commutator subgroup of the group G
$Z_i(G)$	ith term in the upper central series of the group G
$Z_i^p(G)$	ith term in the upper exponent-p-central series of the group G
$K_i(G)$	ith term in the lower central series of the group G
$P_i(G)$	ith term in the lower exponent-p-central series of the group G
G^p	group generated by the pth powers of elements in the group G
$\phi(G)$	Frattini subgroup of the group G
$\mathrm{cl}(G)$	exponent-p-central class of the group G
$\lvert G \rvert$	order of G
$\mathrm{Aut}(G)$	automorphism group of the group G
$\mathrm{Stab}(G)$	stabilizer of the group G
$\langle a_1, \ldots, a_n \rangle$	group generated by the elements $a_1, \ldots, a_n$
$[a, b]$	commutator of the elements a, b
$[a_1, \ldots, a_n]$	simple commutator of the elements $a_1, \ldots, a_n$
$[A, B]$	commutator subgroup generated by the commutators $[a, b]$ of elements a in the group A and b in the group B

C_{p^n}	cyclic group of order p^n
A_d	elementary abelian p-group of rank d
E	identity subgroup
$\mathbf{N}$	natural numbers
(a, b)	greatest common divisor of a, b

CHAPTER 1

INTRODUCTION

The question whether it is possible to determine all groups of a given order up to isomorphism has been dealt with by various people since the beginning of the study of finite groups. A simple but not practical solution can be given using Latin squares. Theoretically it is possible to write down all Latin squares of a given order to check whether they are tables for associative multiplication and finally to arrange them into isomorphism classes. But in practice it is impossible to determine all groups of a given order this way. Furthermore the structure of a group can not be easily extracted from the Latin square.

Research has shown that structural criteria are useful when determining finite groups. An important result in this field of study is that every finite group of order $p^{\alpha}r$, where p is a prime, $\alpha > 0$, and r is not divisible by p, has at least one subgroup of order p^{α} (first Sylow theorem). Furthermore, all such subgroups are isomorphic (second Sylow theorem). Therefore the study of groups of prime power order, generally known as finite p-groups, became one of the basic fields of study in group theory. For the remainder of this chapter the term "p-group" will always denote a finite p-group and isomorphic groups are considered equal.

The earlier works on the classification problem of p-groups dealt with p-groups of small order. Netto [1882] proved that there are only two groups of order p^2. These are the cyclic group of order p^2 and the direct product of two cyclic groups of order p. All groups of order p^3 and p^4 were determined by Young [1893] and Hölder [1893] who independently showed that there are 5 groups of order p^3 and 15 of order

p^4 (14 for $p = 2$). The groups of order p^5, where p is an odd prime, were first classified by Bagnera [1898]. Errors in this list were pointed out by Miller [1899] for order 2^5 (this was corrected by Bagnera [1899]), and by Bender [1927] for order 3^5 (this was not corrected until 1969 by James). All these authors made use of certain characteristics of p-groups of small order, like the presence or absence of an abelian subgroup of index p, the number of independent generators, and the number of inner automorphisms. The major problem of all these approaches is that the criteria used proved insufficient to distinguish isomorphism classes for p-groups of order greater than p^5. The dimension of the task of classifying all p-groups became clearer when G. Higman [1960] and Sims [1965] showed that the number of groups of order p^n approaches $p^{a(n,p)n^3}$ asymptotically where $a(n, p) = 2/27 + O(n^{-1/3})$.

The first systematic attempt to classify p-groups is due to P. Hall [1940]. He uses an equivalence relation which is weaker than isomorphism and points out that it can be applied as an intermediate step when classifying p-groups. As this method is used by James [1969] to determine all p-groups up to order p^6 we will discuss it in more detail.

Let us first recall the definition of a central series. A series of subgroups of a group G, $G = G_0 \geq G_1 \geq \ldots \geq G_n$, with $G_i \trianglelefteq G$, $1 \leq i \leq n$, is called a *central series*[1] if $[G_i, G] \leq G_{i+1}$, $0 \leq i \leq n-1$. There are two particularly important types of central series, the *lower central series* $G = K_1(G) \geq K_2(G) \geq \ldots \geq K_n(G)$ and the *upper central series* $E = Z_0(G) \leq Z_1(G) \leq \ldots \leq Z_n(G)$ where $Z_{i+1}(G)/Z_i(G)$ is the centre

---

[1] The notation in this thesis is based on Huppert [1967] and a page of notation is included at the beginning.

of $G/Z_i(G)$ and E denotes the identity. It is an essential feature of these central series that $K_{r+1}(G) = E$ implies $Z_r(G) = G$ and *vice versa*. Groups for which $G_r = E$ for some r are called *nilpotent*. We define the *nilpotency class* of a nilpotent group to be the smallest integer r for which $K_r(G) \neq E$ and $K_{r+1}(G) = E$. It is a well known fact that a finite group is nilpotent if and only if it is the direct product of p-groups [see Huppert, 1967, Kap. III, 2.3]. Thus, in particular, a p-group has a central series terminating in the identity.

P. Hall [1940] emphasises that "[so] far as prime-power groups are concerned, it will probably be agreed that the most important number associated with the group, after the order, is the class of the group". Therefore he introduces an equivalence relation - isoclinism - that preserves the class. This is defined as follows:

Two groups G, H are *isoclinic* if

(a) $G/Z(G) \cong H/Z(H)$ where $Z(G)$, $Z(H)$ denote the centre of G, H ;

(b) $G' \cong H'$ where G', H' are the commutator subgroups of G, H , respectively;

(c) isomorphisms $\theta : G/Z(G) \to H/Z(H)$ and $\phi : G' \to H'$ may be chosen such that the following diagram commutes:

$$\begin{array}{ccc} G/Z(G) \times G/Z(G) & \xrightarrow{\theta \times \theta} & H/Z(H) \times H/Z(H) \\ \downarrow{\scriptstyle \chi_1} & & \downarrow{\scriptstyle \chi_2} \\ G' & \xrightarrow{\phi} & H' \end{array}$$

where $\big(aZ(G), bZ(G)\big)\theta \times \theta = \big(\big(aZ(G)\theta, \big(bZ(G)\big]\theta\big)$ and χ_1, χ_2 are the canonical maps $\big(aZ(G), bZ(G)\big)\chi_1 = [a, b]$ and similarly for H .

The pair (θ, ϕ) of isomorphisms in (a), (b) is called an *isoclinism*.

The class of all p-groups can be partitioned into isoclinism classes, called *families*. An important fact is that every family contains groups of minimal order, referred to as the *stem groups* of the family. Furthermore a *branch* of a family consists of all those groups in the family which have a given order. Thus to classify all p-groups up to a given order it is first necessary to calculate certain families, then to determine all p-groups up to the desired order in those families, and finally to exclude isomorphic ones. As yet this has only been done for groups of order p^5, $p > 3$, and p-groups which have an abelian subgroup of index p [see P. Hall, 1940], 2-groups up to order 2^6 [see M. Hall and Senior, 1964] and groups of order up to p^6, $p \geq 3$ [see James, 1969][2]. Furthermore the method given by P. Hall is not written in an algorithmic form. Thus it is not clear whether it could be used for computerized calculations.

The procedure used in this thesis for determining all 2-generator p-groups up to order p^6, $p \geq 7$, is an algorithm. It has been computer-implemented at the Australian National University in cooperation with Leedham-Green and his colleagues at Queen Mary College, where an implementation of a related algorithm is available. So far the implementations are only applicable for a fixed prime and fixed number of generators, and soluble automorphism groups.

We will now outline the algorithm we use in this thesis for classifying p-groups. Most of its theoretical background will be discussed in detail and for the proofs omitted references will be given. In the algorithm, a special central series, an *exponent-p-central series*, is used. It is a

---

[2] James has found errors in this list and an unpublished list of corrections is available from him. We will later [see Chapter 6] point out a further discrepancy of our list of groups of order p^6 and the corrected list.

central series with the additional property that every factor has exponent p . The lower and upper exponent-p-central series as well as the exponent-p-central class are defined analogously to the lower and upper central series and the nilpotency class. In Chapter 2 we shall develop a theory for exponent-p-central series that corresponds to that for central series. An advantage of using an exponent-p-central series, when determining p-groups, is that it reflects the commutator and the pth power structure of a group simultaneously. Furthermore a necessary and sufficient condition for a finitely generated group G to be a p-group can be obtained using an exponent-p-central series, namely G is a p-group if and only if it has an exponent-p-central series terminating in the identity.

In Chapter 3 we give some theoretical background of the algorithm. We introduce certain types of group extensions, called *descendants*, and show that every d-generator p-group is a descendant of A_d , the elementary abelian p-group on d generators. We call a descendant Q of a p-group P with exponent-p-central class c an *immediate descendant* of P if Q has exponent-p-central class $c + 1$. Then we introduce the *covering group* P^* of P which has the property that every immediate descendant of P is isomorphic to a factor group of P^* . Furthermore we will show that P has no descendants if the exponent-p-central class of P and P^* are the same. We also prove that, using the automorphism group of P^* , we can give a criterion for two immediate descendants to be isomorphic.

In Chapter 4 we develop methods for constructing the covering group P^* of a p-group P and a subgroup of the automorphism group of P^* - the *covering automorphism group* - which is sufficient to arrange all immediate descendants of P into isomorphism classes. For the construction of the covering group of P a special type of presentation - a *power commutator presentation* - is required for P . We discuss the properties of such a

presentation in some detail. For the construction of the covering automorphism group we rely on a method given by Ascione [1979]. We only outline the procedure and omit proofs. Similarly we only quote her results concerned with the automorphisms of an immediate descendant that are needed to apply the algorithm to it.

Theoretically the constructions given in Chapter 4 together with the results of Chapter 3 yield a method for constructing all p-groups. Of course, in practice computational problems limit the applicability of the algorithm to p-groups of small order. Interesting results for 3-groups are given by Ascione, Havas and Leedham-Green [1977] and for 2-groups and 3-groups by Ascione [1979]. Furthermore the computer implementation of this algorithm and a related one have been used to calculate 5-groups and 7-groups of maximal nilpotency class at the Australian National University and Queen Mary College.

In this thesis we basically restrict the classification problem to the enumeration of all 2-generator p-groups of order up to p^6, $p \geq 7$. For some relatively simple cases descendants up to order p^8 will be given. Furthermore a general description of all descendants of the 2-generator abelian group of order p^3 is given [see Chapter 6].

In Chapter 5 we discuss several methods that are used to simplify computational problems which occur in our calculations. Chapter 6 contains detailed calculations for interesting cases. In particular, we show that according to our computations there are $p - 1$ more 2-generator groups of order p^6 than James [1969] claims. The discrepancy occurs in the families ϕ_{25}, ϕ_{26} [see James, 1969, p. 172, and p. A.29 or in the corrected list p. 40f and p. 75][3].

[3] Also for the case $p = 3$ there seems to be an error in the list given by James, since the list provided by Ascione, Havas, Leedham-Green [1977] contains two more groups [see family G, H in the microfiche supplement] than James claims.

The last chapter contains a list of all 2-generator p-groups of order up to p^6 and some of order p^7, p^8, $p \geq 7$ as well as detailed explanations on how to read the list. The groups are ordered according to their order. We provide a graphical representation of all groups listed that reflects exponent-p-central class and order of the groups listed. Furthermore a special code is used when naming the groups. The code gives the order, exponent-p-central class and the sequence of immediate descendants that is related to the group. We hope this will enable the interested reader to make optimal use of this list.

CHAPTER 2

GROUPS OF PRIME POWER ORDER AND EXPONENT-p-CENTRAL SERIES

The lower central series is used to determine the structure of nilpotent groups. The theory of these groups is well established [see Huppert, 1967, Kap. III]. It is well known that every finite p-group is nilpotent but that the converse is not necessarily true. In this chapter we develop a theory for the exponent-p-central series analogous to that for the central series. The main result is that using the exponent-p-central series, the class of finitely generated groups which have such a series terminating in the identity is the class of finite p-groups. We will not introduce a special name for groups with exponent-p-central series terminating in the identity, since in this thesis we are only interested in finite p-groups.

Firstly note that for a central series defined as in Chapter 1 the assumption $G_i \trianglelefteq G$ is not necessary. Since $[G_i, G] \leq G_{i+1} \leq G_i$ implies $G = N_G(G_i)$, $1 \leq i \leq r-1$, and for every $x \in G_r$, $g \in G$, $x^g = x[x, g]$ and $[x, g] \in [G_{r-1}, G] \leq G_r$, it follows that $G_i \trianglelefteq G$, $1 \leq i \leq r$.

In the following definition G_i^p is the subgroup of G_i generated by the pth powers of the elements of G_i .

DEFINITION 2.1. An *exponent-p-central series* in a group G is a series $G = G_0 \geq G_1 \geq \ldots \geq G_r$ with the following property:

$$[G_i, G]G_i^p \leq G_{i+1} , \quad 0 \leq i \leq r-1 .$$

Again it follows immediately that $G_i \trianglelefteq G$, $1 \leq i \leq r$.

Now we define the p-centre of a group and give a necessary and sufficient condition for a series to be an exponent-p-central series.

DEFINITION 2.2. The *p-centre* $Z^p(G)$ of a group G is the subgroup of $Z(G)$, generated by the elements in $Z(G)$ that have order p.

LEMMA 2.3. *A chain of subgroups* $G = G_0 \geq G_1 \geq \ldots \geq G_r$ *is an exponent-p-central series if and only if each* $G_i \trianglelefteq G$ *and* $G_i/G_{i+1} \leq Z^p(G/G_{i+1})$.

Proof. We may suppose that each $G_i \trianglelefteq G$. Then if $g \in G_i$ we have $gG_{i+1} \in Z^p(G/G_{i+1})$ if and only if $[g, a] \in G_{i+1}$ for all $a \in G$ and $g^p \in G_{i+1}$. Thus $[G_i, G]G_i^p \leq G_{i+1}$ if and only if $G_i/G_{i+1} \leq Z^p(G/G_{i+1})$. □

DEFINITION 2.4. If a group G has an exponent-p-central series $G = G_0 > G_1 > \ldots > G_r = G_{r+1} = \ldots$, then r is called the *length* of the exponent-p-central series. (Here r is the smallest integer for which $G_r = G_{r+1} = \ldots$.)

LEMMA 2.5. *Let* G *be a group with an exponent-p-central series of length* r. *Then every subgroup and factor group of* G *has an exponent-p-central series of length at most* r.

Proof. Let $G = G_0 > G_1 > \ldots > G_r$ be an exponent-p-central series of length r in a group G and S a subgroup of G. Now consider the following series in S:

$$S = S_0 \geq S_1 \geq \ldots \geq S_r \quad \text{where} \quad S_i = G_i \cap S, \quad 0 \leq i \leq r.$$

Every S_i is normal in S since G_i is normal in G. From $S_i \leq G_i$ and $S \leq G$ it follows that $[S_i, S]S^p \leq [G_i, G]G_i^p \leq G_{i+1}$. Clearly $[S_i, S]S_i^p \leq S$. Therefore $[S_i, S]S_i^p \leq G_{i+1} \cap S = S_{i+1}$. Thus the chosen series is an exponent-p-central series of length at most r in S.

Next let N be a normal subgroup of G, and consider the following

series in G/N :

$$G/N = G_0N/N \geq G_1N/N \geq \ldots \geq G_rN/N$$

where G_i is as above. Now

$$[G_iN/N, G/N](G_iN/N)^p = [G_i, G]N/N \cdot G_i^pN/N = [G_i, G]G_i^pN/N \leq G_{i+1}N/N$$

and $G_iN/N \trianglelefteq G/N$ since $G_i \trianglelefteq G$. The chosen series is therefore an exponent-p-central series of length at most r . □

DEFINITION 2.6. The *lower exponent-p-central series* in a group G is the series:

$$G = P_0(G) \geq P_1(G) \geq \ldots \geq P_r(G) \quad \text{where} \quad P_{i+1}(G) = [P_i(G), G]P_i(G)^p .$$

LEMMA 2.7. *The lower exponent-p-central series has the following properties:*

(a) $P_c(G) = P_{c+1}(G)$ *implies* $P_{c+1}(G) = P_{c+2}(G)$;

(b) $P_i(G)/P_{i+1}(G)$ *is an elementary abelian p-group;*

(c) if $\theta : G \to H$ *is a homomorphism of groups then*

$$P_i(G)\theta = P_i(G\theta) ;$$

(d) $P_i(G/N) = P_i(G)N/N$;

(e) $P_i(G)$ *is a fully invariant subgroup of* G .

Proof. *(a)*

$$P_{c+2}(G) = [P_{c+1}(G), G]P_{c+1}(G)^p = [P_c(G), G]P_c(G)^p = P_{c+1}(G) .$$

(b) $P_i(G)/P_{i+1}(G) \leq Z^p\left(G/P_{i+1}(G)\right)$, by Lemma 2.3, hence $P_i(G)/P_{i+1}(G)$ is an elementary abelian p-group.

(c) Proceed by induction on i : for $i = 0$, $P_0(G)\theta = G\theta = P_0(G\theta)$. Suppose $i > 0$ then

$$P_i(G)\theta = \left([P_{i-1}(G), G]P_{i-1}(G)^p\right)\theta = [P_{i-1}(G\theta), G\theta]P_{i-1}(G\theta)^p = P_i(G\theta) .$$

(d) Choose θ in *(c)* to be the canonical homomorphism from G onto G/N then $P_i(G/N) = P_i(G)N/N$ follows immediately from *(c)*.

(e) For every endomorphism ε of G it follows from *(c)* that $P_i(G)\varepsilon = P_i(G\varepsilon)$. Thus $P_i(G)$ is closed under all endomorphisms of G and hence is fully invariant. □

DEFINITION 2.8. The *upper exponent-p-central series* in a group G is the series:

$$E = Z_0^p(G) \leq Z_1^p(G) \leq \ldots \leq Z_r^p(G)$$

where $Z_{i+1}^p(G)$ is the subgroup of G for which

$$Z_{i+1}^p(G)/Z_i^p(G) = Z^p\left(G/Z_i^p(G)\right) , \quad 0 \leq i \leq r-1 .$$

LEMMA 2.9. *If a group G has an exponent-p-central series*

$$G = G_0 \geq G_1 \geq \ldots \geq G_r \text{ and } G_r = E ,$$

then $P_i(G) \leq G_i$ *and* $G_{r-i} \leq Z_i^p(G)$, $0 \leq i \leq r$.

Proof. We will prove the lemma by induction on i . Let $i = 0$ then $E = G_r = Z_0^p(G)$ and $G = G_0 = P_0(G)$. When $i > 0$ we can assume that $P_{i-1}(G) \leq G_{i-1}$ and $G_{r-i+1} \leq Z_{i-1}^p(G)$. Then the first inequality follows from

$$P_i(G) = [P_{i-1}(G), G]P_{i-1}(G)^p \leq [G_{i-1}, G]G_{i-1}^p \leq G_i .$$

Secondly if

$$[G_{r-i}, G]G_{r-i}^p \leq G_{r-i+1} \leq Z_{i-1}^p(G) ,$$

then for all elements in G_{r-i} their commutators with elements of G and their pth powers lie in $Z_{i-1}^p(G)$. But the p-centre of $G/Z_{i-1}^p(G)$ is $Z_i^p(G)/Z_{i-1}^p(G)$. Therefore $G_{r-i} \leq Z_i^p(G)$. □

COROLLARY 2.10. *If G is a group with an exponent-p-central series terminating in the identity then the upper and lower exponent-p-central series have the same length and this is the minimal length of any exponent-p-central series.*

DEFINITION 2.11. A group G has *exponent-p-central class* c if it has a lower exponent-p-central series of length c with $P_c(G) = E$. In the following the class of G, abbreviated $\mathrm{cl}(G)$, always refers to exponent-p-central class.

LEMMA 2.12. *Let G be a group with the lower exponent-p-central series $G = P_0(G) \geq P_1(G) \geq \ldots \geq P_r(G)$. Then*

(a) $G/P_i(G)$ has class at most i;

(b) if $G/P_i(G)$ has class i, then $G/P_{i-1}(G)$ has class $i - 1$;

(c) if G/N has class i, then $P_i(G) \leq N$ and $P_{i-1}(G) \not\leq N$.

Proof. *(a)* $P_i\left(G/P_i(G)\right) = P_i(G)/P_i(G) = E$ by Lemma 2.7 *(d)*.

(b) Let $G/P_i(G)$ have class i. By *(a)* the class of $G/P_{i-1}(G)$ is at most $i - 1$. Now suppose $\mathrm{cl}\left(G/P_{i-1}(G)\right) < i - 1$ then $P_{i-2}\left(G/P_{i-1}(G)\right) = E$. But

$$P_{i-2}\left(G/P_{i-1}(G)\right) = P_{i-2}(G)P_{i-1}(G)/P_{i-1}(G) = P_{i-2}(G)/P_{i-1}(G).$$

Hence $P_{i-2}(G) = P_{i-1}(G)$. Now it follows from Lemma 2.7 *(a)* that $P_i(G) = P_{i-1}(G)$ and therefore $G/P_i(G)$ has class at most $i - 1$, a contradiction.

(c) Let G/N have class i. Then $P_i(G/N) = E$ and $P_{i-1}(G/N) \neq E$. But $E = P_i(G/N) = P_i(G)N/N$ and $E \neq P_{i-1}(G/N) = P_{i-1}(G)N/N$ by Lemma 2.7 *(d)*. Therefore $P_i(G) \leq N$ and $P_{i-1}(G) \not\leq N$.

PROPOSITION 2.13. *Every finite p-group has an exponent-p-central series terminating in the identity.*

Proof. Let G be a finite p-group of order p^n. We shall prove the proposition by induction on n. The cases $n = 0, 1$ are trivial. Now let $n > 1$. It is well known that $Z(G)$ is non-trivial [see Huppert, 1967, Kap. I, 6.9] and hence $Z^p(G)$ is non-trivial. Therefore we can assume that $G/Z^p(G)$ has an exponent-p-central series:

$$G/Z^p(G) = G_0/Z^p(G) \geq \ldots \geq G_r/Z^p(G) = E$$

and

$$\left[G_i/Z^p(G),\ G/Z^p(G)\right]\left(G_i/Z^p(G)\right)^p \leq G_{i+1}/Z^p(G)\ ,\quad 0 \leq i \leq r\text{-}1\ .$$

Thus $[G_i, G]G_i^p \leq G_{i+1}Z^p(G) = G_{i+1}$ and each $G_i \trianglelefteq G$, $1 \leq i \leq r$. Then the series $G = G_0 \geq G_1 \geq \ldots \geq G_r = Z^p(G) \geq E$ is an exponent-p-central series for G terminating in the identity. □

The following theorem has as a corollary the main result of this chapter.

THEOREM 2.14. *If G is a finitely generated group then $G/P_i(G)$ is a finite p-group.*

Proof. The proof goes by induction on i. Let G be generated by $\{g_1, \ldots, g_d\}$ then $G/P_1(G)$ is generated by $\{g_1P_1(G), \ldots, g_dP_1(G)\}$. But $G/P_1(G)$ is an elementary abelian p-group by Lemma 2.7 *(b)*. Thus $|G/P_1(G)| \leq p^d$.

Suppose $i > 1$ then we can assume that $G/P_{i-1}(G)$ is a finite p-group. As $P_{i-1}(G)$ is a subgroup of G with finite index $P_{i-1}(G)$ is finitely generated [see Huppert, 1967, Kap. I, 19.10]. Therefore

$P_{i-1}(G)/P_1(P_{i-1}(G))$ is a finite elementary abelian p-group. Now

$$P_1(P_{i-1}(G)) = [P_{i-1}(G), P_{i-1}(G)]P_{i-1}(G)^p \leq [P_{i-1}(G), G]P_{i-1}(G)^p = P_i(G) ;$$

hence $P_{i-1}(G)/P_i(G)$ is a finite elementary abelian p-group. Since $G/P_{i-1}(G)$ and $P_{i-1}(G)/P_i(G)$ are finite p-groups and

$$|G/P_i(G)| = [G : P_{i-1}(G)][P_{i-1}(G) : P_i(G)] ,$$

$G/P_i(G)$ is a finite p-group. □

COROLLARY 2.15. *A group is a finite p-group if and only if it is finitely generated and has the lower exponent-p-central series terminating in the identity.*

Proof. Suppose G is a finitely generated group and has the lower exponent-p-central series

$$G = P_0(G) \geq P_1(G) \geq \ldots \geq P_r(G) = E .$$

Then it follows from Theorem 2.14 that $G/P_r(G) \cong G$ is a finite p-group. The converse holds by Proposition 2.13.

DEFINITION 2.16. The *Frattini subgroup* $\phi(G)$ of a group G is the intersection of all the maximal subgroups of G and $\phi(G) = G$ if G has no maximal subgroups.

DEFINITION 2.17. A subset of a group G is *omissible* if it can be omitted from every generating set for G .

LEMMA 2.18. *In every finitely generated group G with the lower exponent-p-central series terminating in the identity, $P_i(G)$ is omissible for $1 \leq i \leq cl(G)$.*

Proof. Since G is a finite p-group by Theorem 2.14, $P_1(G) = \phi(G)$ [see B. Huppert, 1967, Kap. III, 3.14]. Therefore $P_i(G) \leq P_1(G) = \phi(G)$ is omissible for $1 \leq i \leq cl(G)$ [see B. Huppert, 1967, Kap. III, 3.2].

CHAPTER 3

DESCENDANTS OF A p-GROUP

In this chapter we will develop a theory for certain extensions of a group called descendants [see 3.2]. An important result is that every d-generator p-group is a descendant of the elementary abelian p-group on d generators. We will classify all descendants of a p-group up to isomorphism. In the next chapter a method of constructing these descendants will be given. This is based on a procedure described by M.F. Newman [1975]; more detailed discussion of it can be found in Ascione [1979]. The procedure itself will be referred to as "the algorithm".

Throughout this chapter F will be the free group freely generated by $\{a_1, \ldots, a_d\}$ and P will always denote a finite p-group on exactly d generators. Firstly, we give the definition of an extension of a group.

DEFINITION 3.1. A group G is an *extension* of a group A by a group B if G has a normal subgroup N with

$$N \cong B \quad \text{and} \quad G/N \cong A \ .$$

DEFINITION 3.2. A group Q is a *descendant* of P if for some r, $P \cong Q/P_r(Q)$ and $P_r(Q)$ is non-trivial. The group Q is an *immediate descendant* of P if $\mathrm{cl}(P) = r$ and $\mathrm{cl}(Q) = r + 1$.

LEMMA 3.3. *If P has class c then there exists a sequence of groups Q_i of length $c + 1$: $Q_0, Q_1, \ldots, Q_c$ where $Q_0 \cong E$ and $Q_c \cong P$ with the following properties:*

$$\mathrm{cl}(Q_i) = i \quad \textit{and} \quad Q_i/P_{i-1}(Q_i) \cong Q_{i-1} \ .$$

Proof. Since $\mathrm{cl}(P) = c$ it has a lower exponent-p-central series

$$P = P_0(P) \geq P_1(P) \geq \ldots \geq P_c(P) = E \quad \text{with} \quad P_{c-1}(P) \neq E \ .$$

Now let Q_i be $P/P_i(P)$. Then by Lemma 2.12, $cl(Q_i) = cl(P/P_i(P)) \leq i$, $0 \leq i \leq c$. But $P_{i-1}(P/P_i(P)) = P_{i-1}(P)/P_i(P) \neq E$, $0 < i \leq c$, since P has class c . Therefore $cl(Q_i) = i$.

Also

$$\begin{aligned} Q_i/P_{i-1}(Q) &= (P/P_i(P))/(P_{i-1}(P/P_i(P))) \\ &= (P/P_i(P))/(P_{i-1}(P)P_i(P)/P_i(P)) \text{ by Lemma 2.7 } (d) \\ &\cong P/P_{i-1}(P) = Q_{i-1} \text{ since } P_i(P) \leq P_{i-1}(P) . \quad \square \end{aligned}$$

COROLLARY 3.4. *If P has class c , $c \geq 2$, then it is a descendant of the elementary abelian p-group A_d on d generators and also an immediate descendant of a d-generator p-group Q of class $c - 1$. Furthermore if $P \cong F/R$ for a normal subgroup R of G , then $R \leq P_1(F)$.*

Proof. Since P is a descendant of Q_1 and a d-generator p-group

$$Q_1 = P/P_1(P) = P/\Phi(P) \cong A_d .$$

Now let Q be Q_{c-1} . P is an immediate descendant of Q , since

$$Q = P/P_{c-1}(P) \text{ and } cl(Q) = cl(Q_{c-1}) = c - 1 .$$

Let $P \cong F/R$ for a normal subgroup R of F . Then

$$F/P_1(F) \cong A_d \cong P/P_1(P) \cong (F/R)/(P_1(F)R/R) \cong F/P_1(F)R ,$$

so $P_1(F)R = P_1(F)$ and thus $R \leq P_1(F)$. $\square$

LEMMA 3.5. *Every descendant Q of P is again a d-generator p-group.*

Proof. Let $\{b_1, \ldots, b_d\}$ generate P and let $Q/P_r(Q) \cong P$. Now choose elements $q_1, \ldots, q_d$ in Q such that $q_i\rho = b_i$ where ρ is an epimorphism that maps Q onto P with kernel $P_r(Q)$. Thus $\{q_1, \ldots, q_d\} \cup P_r(Q)$ generates Q . Since $P_r(Q)$ is omissible by

Corollary 2.15, $\{q_1, \ldots, q_d\}$ generates Q. □

LEMMA 3.6. *Let P have class c and choose a normal subgroup R of F such that $P \cong F/R$. Then a d-generator p-group Q is an immediate descendant of P if and only if $Q \cong F/M$ for some normal subgroup M of F satisfying:*

$$P_c(F)M = R\ ,\quad P_{c+1}(F) \leq M\ ,\quad P_c(F) \nleq M\ .$$

In particular, M is a proper supplement of $P_c(F)$ in R.

Proof. Suppose first that M is a normal subgroup of F satisfying:

$$P_c(F)M = R\ ,\quad P_{c+1}(F) \leq M\ ,\quad P_c(F) \nleq M$$

and let $Q \cong F/M$. Then

$$P \cong F/R = F/P_c(F)M \cong (F/M)/\left(P_c(F)M/M\right) = (F/M)/P_c(F/M) \cong Q/P_c(Q)\ .$$

Therefore Q is a descendant of P.

Now $P_c(F) \nleq M$ and $P_{c+1}(F) \leq M$ imply that

$$P_c(Q) \cong P_c(F/M) = P_c(F)M/M \neq E$$

and

$$P_{c+1}(Q) \cong P_{c+1}(F)M/M = E\ .$$

Thus Q has class $c + 1$ and is an immediate descendant of P.

Conversely, suppose Q has class $c + 1$ and is an immediate descendant of P. Since $P \cong F/R$ and $P \cong Q/P_c(Q)$ there exist epimorphisms $\theta : F \to P$ and $\rho : Q \to P$ with $\ker \theta = R$ and $\ker \rho = P_c(Q)$. Because Q is a d-generator p-group by Lemma 3.5 and F is the free group on d generators, we may choose an epimorphism $\psi : F \to Q$ satisfying $a_i\theta = a_i\psi\rho$ and thus get $\psi\rho = \theta$. Now set $\ker \psi = M$.

If $w \in M$, then $w\theta = w\psi\rho = e$, so $w \in \ker \theta = R$, and therefore $M \leq R$. Thus $P_c(F)M \leq R$ since P has class c, and because

$$F/R \cong P \cong Q/P_c(Q) \cong (F/M)/\{P_c(F)M/M\} \cong F/P_c(F)M ,$$

we in fact have $P_c(F)M = R$.

Furthermore, $\mathrm{cl}(Q) = c + 1$ and $Q \cong F/M$ yield $P_{c+1}(F) \leq M$ and $P_c(F) \not\leq M$. □

Now we will introduce a d-generator p-group P^* such that every immediate descendant of $P \cong F/R$ is isomorphic to a factor group of P^* and furthermore, to within isomorphism, P^* is independent of the choice of R .

DEFINITION 3.7. Let $P \cong F/R$ and $R^* = [R, F]R^p$ which is a normal subgroup of F . Then the group $P^* = F/R^*$ is the *covering group* of P and R/R^* is the *p-multiplicator* of P .

LEMMA 3.8. *The group P^* is a finite d-generator p-group of class at most $c + 1$.*

Proof. Let $P \cong F/R$ and $P^* = F/R^*$ be the covering group of P . Then $P_c(F) \leq R$ implies

$$P_{c+1}(F) = [P_c(F), F](P_c(F))^p \leq [R, F]R^p = R^* .$$

Now F has rank d , therefore by Theorem 2.14, $F/P_{c+1}(F)$ is a finite d-generator p-group.

Because $F/R^* \cong \{F/P_{c+1}(F)\}/\{R^*/P_{c+1}(F)\}$ and $P_{c+1}(F) \leq R^*$ it follows that F/R^* is a finite d-generator p-group of class at most $c + 1$. □

LEMMA 3.9. *The covering group of P is determined up to isomorphism by the group P .*

Proof. Suppose $\theta_1, \theta_2 : F \to P$ are epimorphisms, with $\ker \theta_1 = R_1$ and $\ker \theta_2 = R_2$, and let $P_1^* = F/R_1^*$, $P_2^* = F/R_2^*$ be covering groups for P .

Consider the isomorphism $P_1^*/(R_1/R_1^*) \cong F/R_2$ given by

$$P_1^*/(R_1/R_1^*) = (F/R_1^*)/(R_1/R_1^*) \cong F/R_1 \cong P \cong F/R_2 .$$

Because $R_1 \leq P_1(F)$, R_1/R_1^* is omissible in P_1^*. Applying an argument like that in Lemma 3.5, one can show that there exists a generating set $\{q_1, \ldots, q_d\}$ of P_1^* and an epimorphism $\rho : P_1^* \to F/R_2$ satisfying $\ker \rho = R_1/R_1^*$ and $q_i\rho = a_i\theta_2$, $1 \leq i \leq d$.

Let $\psi : F \to P_1^*$ be the epimorphism determined by $a_i\psi = q_i$, $1 \leq i \leq d$. Then $\psi\rho = \theta_2$. Set $M = \ker \psi$.

We have $R_2\psi\rho = R_2\theta_2 = E$; thus $R_2\psi \leq \ker \rho = R_1/R_1^*$. But $R_1/R_1^* \leq Z^p(F/R_1^*)$; hence

$$R_2^*\psi = \left([R_2, F]R_2^p\right)\psi \leq [R_1/R_1^*, F/R_1^*](R_1/R_1^*)^p = E .$$

Thus $R_2^* \leq \ker \psi = M$. Therefore $P_1^* \cong F/M \cong (F/R_2^*)/(M/R_2^*)$ is a homomorphic image of P_2^*. Similarly P_2^* can be shown to be a homomorphic image of P_1^*, and because P_1^*, P_2^* are finite by Lemma 3.8, we have $P_1^* \cong P_2^*$. □

It is now convenient to take a standard representation for P, namely F/R.

THEOREM 3.10. *Every immediate descendant of P is isomorphic to a factor group of the covering group of P.*

Proof. Let P have class c and Q be an immediate descendant of P. Choose the epimorphisms θ, ψ, ρ as in the second half of the proof of Lemma 3.6. Then $R\psi\rho = R\theta = E$, so $R\psi \leq \ker \rho = P_c(Q)$. On the other hand $R\psi = R/M$, so that $\mathrm{cl}(F\psi/R\psi) = \mathrm{cl}(F/R) = c$ and by Lemma 2.12 *(c)*, $P_c(Q) = P_c(F\psi) \leq R\psi$. Therefore $R\psi = P_c(Q)$. Now it follows from

$$R^*\psi = [R\psi, F\psi](R\psi)^p = [P_c(Q), Q]P_c(Q)^p = P_{c+1}(Q) = E ,$$

that $R^* \leq \ker \psi = M$ and $Q \cong F/M \cong (F/R^*)/(M/R^*)$. Thus every immediate descendant of P is isomorphic to a factor group of the covering group P^* . □

DEFINITION 3.11. The *nucleus* of a group P of class c is $P_c(P^*)$. Since $P_c(P^*) = P_c(F)R^*/R^*$ and $P_c(F)$, $R^* \leq R$ we may talk of supplements of the nucleus in the p-multiplicator.

DEFINITION 3.12. An *allowable subgroup* of the p-multiplicator is a proper supplement of the nucleus in the p-multiplicator.

LEMMA 3.13. *If Q is an immediate descendant of P , then there exists an allowable subgroup M/R^* such that $Q \cong F/M$ and if M/R^* is an allowable subgroup then $Q \cong F/M$ is an immediate descendant of P .*

Proof. If Q is an immediate descendant of P then by Lemma 3.6 and the proof of Theorem 3.10, there exists a normal subgroup M of F such that $Q \cong F/M$ satisfying:

$$P_c(F)M = R \ , \quad P_{c+1}(F) \leq M \ , \quad P_c(F) \nleq M \quad \text{and} \quad R^* \leq M \ .$$

Thus

$$R/R^* = P_c(F)M/R^* = P_c(F)R^*/R^* \ . \ M/R^* \ ,$$

$$P_{c+1}(F)R^*/R^* \leq M/R^* \ ,$$

and

$$P_c(F)R^*/R^* \nleq M/R^* \ .$$

Therefore M/R^* is an allowable subgroup.

If M/R^* is an allowable subgroup then it follows immediately by Lemma 3.6 and the proof of Theorem 3.10 that $Q \cong F/M$ is an immediate descendant of P . □

LEMMA 3.14. *A group P of class c has descendants if and only if its covering group has class $c + 1$.*

Proof. Firstly, let Q be an immediate descendant of P . Then

$Q \cong F/M$ with M as in the proof of Lemma 3.13; in particular $P_c(F) \nleq M$. Now $R^* \leq M$ implies $P_c(F) \nleq R^*$. Therefore $\mathrm{cl}(P^*) = \mathrm{cl}(F/R^*) > c$. But by Lemma 3.8, $\mathrm{cl}(F/R^*) \leq c + 1$; hence $\mathrm{cl}(F/R^*) = c + 1$.

Conversely, let $\mathrm{cl}(P^*) = c + 1$. Then $P_c(F) \nleq R^*$ and $P_{c+1}(F) \leq R^*$. Also, R/R^* is non-trivial, since otherwise $F/R^* \cong (F/R^*)/(R/R^*) \cong F/R$ implies $\mathrm{cl}(F/R^*) = c$, a contradiction. Because R/R^* is elementary abelian, there exists a proper supplement M/R^* of $P_c(F)R^*/R^*$ in R/R^*. Then $P_{c+1}(F) \leq R^* \leq M$ and $Q \cong F/M$ is an immediate descendant of P. □

COROLLARY 3.15. *A group P has descendants if and only if the nucleus of P is non-trivial.*

Proof. The corollary follows immediately from Lemma 3.14 and Lemma 3.13. □

The above description of the immediate descendants of a p-group does not distinguish isomorphism types. The following proposition gives a criterion for distinguishing isomorphic descendants.

PROPOSITION 3.16. *Two allowable subgroups M/R^* and N/R^* give isomorphic descendants F/M and F/N of a group P if and only if there exists an automorphism α of F/R^* such that $(M/R^*)\alpha = N/R^*$.*

Proof. Suppose P has class c. Because F/M, F/N are immediate descendants of P, we have $\mathrm{cl}(F/M) = \mathrm{cl}(F/N) = c + 1$, $P_{c+1}(F) \leq M, N$ and $MP_c(F) = NP_c(F) = R$.

Now suppose $\theta : F/M \to F/N$ is an isomorphism and set $(a_iM)\theta = b_iN$ for some $b_i \in F$. We construct the required automorphism of F/R^*.

To begin with, let ε be the endomorphism of F satisfying $a_i\varepsilon = b_i$, $1 \leq i \leq d$. Clearly we have $M\varepsilon \leq N$. Now $P_{c+1}(F)$ is a fully invariant subgroup of F, so ε induces an endomorphism $\bar{\varepsilon}$ of $F/P_{c+1}(F)$

satisfying $(a_i P_{c+1}(F))\bar{\varepsilon} = b_i P_{c+1}(F)$. Then $\bar{\varepsilon}$ is an automorphism. To see this, it suffices to show that $F/P_{c+1}(F)$ is generated by $\{b_1 P_{c+1}(F), \ldots, b_d P_{c+1}(F)\}$, because $F/P_{c+1}(F)$ is finite.

From the canonical isomorphism $F/N \cong (F/P_{c+1}(F))/(N/P_{c+1}(F))$ we have $F/P_{c+1}(F)$ is generated by

$$\{b_1 P_{c+1}(F), \ldots, b_d P_{c+1}(F)\} \cup N/P_{c+1}(F) .$$

However, $N \leq P_1(F)$ by Corollary 3.4, therefore

$$N/P_{c+1}(F) \leq P_1(F)/P_{c+1}(F) = P_1(F/P_{c+1}(F))$$

is omissible. Thus $F/P_{c+1}(F)$ is generated by $\{b_1 P_{c+1}(F), \ldots, b_d P_{c+1}(F)\}$ as claimed.

Now

$$(R/P_{c+1}(F))\bar{\varepsilon} = (MP_c(F)/P_{c+1}(F))\bar{\varepsilon} \leq NP_c(F)/P_{c+1}(F) = R/P_{c+1}(F)$$

and so $(R/P_{c+1}(F))\bar{\varepsilon} = R/P_{c+1}(F)$ since $R/P_{c+1}(F)$ is finite and $\bar{\varepsilon}$ is an automorphism of $F/P_{c+1}(F)$. Thus

$$(R^*/P_{c+1}(F))\bar{\varepsilon} = \left([R/P_{c+1}(F), F/P_{c+1}(F)](R/P_{c+1}(F))^p\right)\bar{\varepsilon} = R^*/P_{c+1}(F) .$$

Therefore $\bar{\varepsilon}$ induces an automorphism $\bar{\bar{\varepsilon}}$ of F/R^* satisfying $(a_i R^*)\bar{\bar{\varepsilon}} = b_i R^*$ and $(M/R^*)\bar{\bar{\varepsilon}} = N/R^*$. The automorphism $\bar{\bar{\varepsilon}}$ is that required.

Conversely, let α be an automorphism of F/R^* such that $(M/R^*)\alpha = N/R^*$. Then

$$F/N \cong (F/R^*)/(N/R^*) \cong (F/R^*)\alpha/(M/R^*)\alpha \cong (F/R^*)/(M/R^*) \cong F/M .$$

Thus F/N and F/M are isomorphic immediate descendants of P . □

CHAPTER 4

p-COVERING ALGORITHM

In this chapter we construct the covering group F/R^* for P, again representing P as F/R, and a subgroup of $\mathrm{Aut}(F/R^*)$ from $\mathrm{Aut}(F/R)$ which is sufficient to arrange immediate descendants of P into isomorphism classes. This together with the results of Chapter 3 gives a method - the *p-covering algorithm* - for calculating all d-generator p-groups which are descendants of the elementary abelian p-group on d generators.

4.1. Power commutator presentations

DEFINITION 4.1. A *power commutator presentation* of a group has the following form:

$$\left\langle a_1, \ldots, a_n;\ a_i^p = \prod_{k=i+1}^{n} a_k^{\alpha(i,k)},\ [a_j, a_i] = \prod_{k=j+1}^{n} a_k^{\alpha(i,j,k)},\ j > i \right\rangle$$

where $\alpha(i, k)$, $\alpha(i, j, k)$ are integers with $0 \le \alpha(i, k)$, $\alpha(i, j, k) < p$.

In the following $\mathbb{P}_n$ will denote a power commutator presentation on n generators $a_1, \ldots, a_n$.

DEFINITION 4.2. A word w in the group given by $\mathbb{P}_n$ is a *normal word* if

$$w = \prod_{i=1}^{n} a_i^{\beta(i)}, \quad 0 \le \beta(i) < p.$$

PROPOSITION 4.3. *Every element of the group given by* $\mathbb{P}_n$ *can be presented by a normal word.*

Proof. Let G be the group given by $\mathbb{P}_n$. Every element g in G

can be written as a product of powers of a_i , $1 \le i \le n$. We now proceed by induction. The case $n = 1$ is trivial. If $n > 1$, then $a_n \in Z^p(G)$. Then $G/\langle a_n \rangle$ has $n - 1$ generators and

$$g\langle a_n \rangle = \prod_{i=1}^{n-1} a_i^{\beta(i)} \langle a_n \rangle \ , \quad 0 \le \beta(i) < p \ ,$$

by induction. Since a_n is central and has order p ,

$$g = \prod_{i=1}^{n} a_i^{\beta(i)} \ , \quad 0 \le \beta(i) < p \ . \qquad \square$$

In practice one needs an algorithm for normalizing words in a group given by a power commutator presentation [for such an algorithm see M.F. Newman, 1976, or Havas and Nicholson, 1976]. The process of normalizing a word is usually referred to as *collection*.

PROPOSITION 4.4. *The group given by* $\mathbb{P}_n$ *is a* p*-group of order at most* p^n .

Proof. We prove the proposition by induction on n . Let G be the group given by $\mathbb{P}_n$. If $n = 1$, G is cyclic of order p . Now if $n > 1$, then $a_n \in Z^p(G)$. Therefore $\langle a_n \rangle$ is either cyclic of order p or the identity, and normal in G . Thus $G/\langle a_n \rangle$ has $n - 1$ generators and by the induction hypothesis, $|G/\langle a_n \rangle| \Big| p^{n-1}$. Hence

$$|G| = |G/\langle a_n \rangle| \, |\langle a_n \rangle| \Big| p^n \ . \qquad \square$$

PROPOSITION 4.5. *Every* p*-group has a power commutator presentation.*

Proof. Let P have order p^n . By Proposition 2.13, P has the lower exponent-p-central series:

$$P = P_0(P) \ge P_1(P) \ge \ldots \ge P_c(P) = E \quad \text{where} \quad c = \mathrm{cl}(P) \ .$$

This series can be refined to a central series of length n ,

$$P = G_0 > G_1 > \ldots > G_n = E$$

where every factor has order p [see Huppert, 1967, Kap. III, 7.2]. In particular there exist elements $a_1, \ldots, a_n$ in P such that

(1) $G_i = \langle a_{i+1}, G_{i+1} \rangle$, $a_{i+1}^p \in G_{i+1}$,

(2) $[a_j, a_k] \in G_{j+1}$ for all $a_j \in G_j$ and $1 \leq k < n$.

To see this we may suppose $P_{i+1}(P) \leq G_{j+1} < G_j \leq P_i(P)$ for some i , $0 \leq i \leq c\text{-}1$, then

$$[G_j, G_0] = [G_j, P] \leq [P_i(P), P] \leq P_{i+1}(P) \leq G_{j+1}$$

and

$$G_j^p \leq P_i(P)^p \leq P_{i+1}(P) \leq G_{j+1} .$$

Furthermore the definition of $G_0, \ldots, G_n$ guarantees that a_{i+1}^p, $[a_j, a_k]$ can be presented by normal words in G_{i+1}, G_{j+1} , respectively. Thus

$$\left\langle a_1, \ldots, a_n; a_i^p = \prod_{k=i+1}^{n} a_k^{\alpha(i,k)}, [a_j, a_i] = \prod_{k=j+1}^{n} a_k^{\alpha(i,j,k)}, j > i \right\rangle$$

where $\alpha(i, k)$, $\alpha(i, j, k)$ are integers with $0 \leq \alpha(i, j)$, $\alpha(i, j, k) < p$ is a power commutator presentation for P . □

DEFINITION 4.6. If the group presented by a power commutator presentation on n generators has order p^n , then the presentation is *consistent*.

DEFINITION 4.7. A generator a_k is *redundant* if it also can be presented by a normal word

$$\prod_{i=k+1}^{n} a_i^{\beta(i,k)} .$$

PROPOSITION 4.8. *A power commutator presentation is consistent if and only if none of the generators is redundant.*

Proof. We may suppose that P is presented by a power commutator presentation $\mathbb{P}_n$. Then $|P| = p^n$ if and only if the series $E = G_n \leq G_{n-1} \leq \ldots \leq G_0 = P$, where $G_i = \langle a_{i+1}, \ldots, a_n \rangle$ is a central series where every factor has order p. Now by definition, a generator a_k is redundant if and only if $G_k = G_{k-1}$, which is equivalent to $G_{k-1}/G_k = E$. □

Therefore if P is presented by $\mathbb{P}_n$, which is not consistent, some of the generators in $\mathbb{P}_n$ are redundant. Then a presentation in which we successively eliminate all redundant generators by replacing them with the normal words they are equal to, and then normalizing the new words so obtained, is also a power commutator presentation. Furthermore, by Proposition 4.8, the presentation is consistent.

The following theorem gives a method using collection for checking whether a power commutator presentation is consistent.

THEOREM 4.9. *A power commutator presentation on n generators is consistent if and only if the following words*

$$a_k a_j a_i , \quad 1 \leq i < j < k \leq n ,$$

$$\left.\begin{matrix} a_j^p a_i \\ a_j a_i^p \end{matrix}\right\} , \quad 1 \leq i < j \leq n ,$$

$$a_i^p a_i , \quad 1 \leq i \leq n-1 ,$$

when collected in two essentially different ways give the same normal word.

The essentially different ways of collecting are as follows. Brackets indicate the subword to be replaced first:

$$(a_k a_j) a_i \quad \text{and} \quad a_k (a_j a_i) ,$$

$$\left(a_j^p\right) a_i \quad \text{and} \quad a_j^{p-1} (a_j a_i) ,$$

$$(a_j a_i) a_i^{p-1} \quad \text{and} \quad a_j \left[a_i^p \right] ,$$

$$\left[a_i^p \right] a_i \quad \text{and} \quad a_i \left[a_i^p \right] .$$

Collecting these words is referred to as performing consistency checks. A proof of this theorem can be found in Wamsley [1974].

Thus to make a power commutator presentation consistent, it is sufficient to perform consistency checks for the words mentioned in Theorem 4.9 and replace resulting redundant generators as previously described.

We will now introduce a special type of consistent power commutator presentation. The special feature is that if $\mathbb{P}_n$ is consistent and it presents a d-generator p-group, then every a_i, $d+1 \leq i \leq n$, in $\mathbb{P}_n$ is equal to a pth power or a commutator of earlier generators. The corresponding relations in $\mathbb{P}_n$ are called *definitions*.

Now let $\mathbb{P}_n$ be such a presentation then we define a *weight* function on words in $\mathbb{P}_n$ as follows:

(a) $\mathrm{wt}(a_i) = 1$, $1 \leq i \leq d$, $\mathrm{wt}(e) = \infty$,

(b) $\mathrm{wt}(a_k) = \mathrm{wt}(a_j) + 1$ if $a_k = a_j^p$, $d+1 \leq k \leq n$,

(c) $\mathrm{wt}(a_k) = \mathrm{wt}(a_j) + \mathrm{wt}(a_r)$ if $a_k = [a_j, a_r]$, $d+1 \leq k \leq n$,

(d) $\mathrm{wt}\left(\prod_{i=1}^{n} a_i^{\beta(i)} \right) = \mathrm{wt}(a_j)$, if $a_j^{\beta(j)}$ is the first non-trivial term in $\prod_{i=1}^{n} a_i^{\beta(i)}$, $0 \leq \beta(i) < p$;

(e) if w is a non-normal word then $\mathrm{wt}(w)$ is the weight of the normal word to which w is equal.

Clearly for a d-generator p-group P of order p^n and class c, there exists a consistent power commutator presentation $\mathbb{P}_n$ in which the generators are ordered according to the weight function. Obviously the

generators a_j with $wt(a_j) \geq i$ generate $P_{i-1}(P)$. The advantage of such a presentation is that it reflects the sequence of immediate descendants of the group P, since $P/P_i(P) = P/\langle a_j, \ldots, a_n \rangle$ with $wt(a_j) \geq i+1$.

4.2. Construction of the covering group

Since $P = F/R$ and its covering group F/R^* are finite d-generator p-groups by Lemma 3.8, Proposition 4.5 guarantees that they have consistent power commutator presentations $\mathbb{P}_n$ and $\mathbb{P}_{n^*}$, respectively. Now let P be given by a $\mathbb{P}_n$ such that a_j, $d+1 \leq j \leq n$, are given by definitions and ordered according to the weight function. Then we construct $\mathbb{P}_{n^*}$ as follows.

Let F be the free group generated by $c_1, \ldots, c_d$. We may suppose that for the first d generators in $\mathbb{P}_n$, $a_i = c_i R$. All remaining generators a_j, $d+1 \leq j \leq n$, are given by definitions $a_j = w_j(a_1, \ldots, a_d)$ where $w_j(a_1, \ldots, a_d)$ denotes a word in $a_1, \ldots, a_d$. Now put $c_j = w_j(c_1, \ldots, c_d)$. Then $a_j = c_j R$ since R is a normal subgroup of F. Now there are $n + \binom{n}{2}$ relations in $\mathbb{P}_n$ of which $n - d$ are definitions. Thus there are $d + \binom{n}{2}$ relations in $\mathbb{P}_n$ which are not definitions. Then, using Tietze transformations, F/R can be presented by

$$\left\langle c_1 R, \ldots, c_d R; u_j R = v_j R, 1 \leq j \leq d+\binom{n}{2} \right\rangle$$

where $u_j R = v_j R$ replace the relations in $\mathbb{P}_n$ which are not definitions. Furthermore, R is the normal closure of $\left\{u_j v_j^{-1} : 1 \leq j \leq d+\binom{n}{2}\right\}$ and R^*

is the normal closure of

$$\left\{\left[u_j v_j^{-1}, c_i\right], \left(u_j v_j^{-1}\right)^p : 1 \le j \le d+\binom{n}{2}\right\} .$$

Thus F/R^* can be presented by

$$\left\langle c_1 R^*, \ldots, c_d R^*; \left[u_j v_j^{-1}, c_i\right] R^* = R^*, \left(u_j v_j^{-1}\right)^p R^* = R^*, \right.$$
$$\left. 1 \le j \le d+\binom{n}{2}, 1 \le i \le d \right\rangle .$$

Now Tietze transformations are performed to change this presentation into a power commutator presentation on $b_1, \ldots, b_m$ where $m = n + d + \binom{n}{2}$ such that $c_j R^* = b_j$, $1 \le j \le n$. To do this set $b_i = c_i R^*$, $1 \le i \le d$. Then, since $c_j = w_j(c_1, \ldots, c_d)$, $d+1 \le j \le n$, and R^* is normal in F, we can set $b_j = w_j(b_1, \ldots, b_d)$. Thus b_j, $1 \le j \le n$, has the same definition and weight as the corresponding a_j. Therefore the b_j are ordered according to the weight function, and if $\mathrm{cl}(P) = c$, then $\mathrm{wt}(b_j) \le c$. Clearly none of the b_j are redundant since the corresponding a_j are not redundant. The remaining generators b_k, $n+1 \le k \le m$ are defined by the relators $u_j v_j^{-1}$, $1 \le j \le d+\binom{n}{2}$. Thus, if $c_k = w_k(c_1, \ldots, c_d) = u_j v_j^{-1}$, $n+1 \le k \le m$, $1 \le j \le d+\binom{n}{2}$, then $b_k = w_k(b_1, \ldots, b_d)$. Every such b_k is central and has order p since $R/R^* \le Z^p(F/R^*)$. Therefore

$$\left\langle b_1, \ldots, b_m; b_i^p = \prod_{k=i+1}^{m} b_k^{\alpha(i,k)}, [b_j, b_i] = \prod_{k=j+1}^{m} b_k^{\alpha(i,j,k)}, j > i \right\rangle$$

where $\alpha(i, k)$, $\alpha(i, j, k)$ are fixed integers, $0 \le \alpha(i, k)$, $\alpha(i, j, k) < p$, is a power commutator presentation for F/R^*. Note that the generators b_k, $n+1 \le k \le m$ are not necessarily given by definitions.

But we will show later that the ones which remain in the presentations of immediate descendants are given by definitions. This presentation is not necessarily consistent. Since b_j , $1 \le j \le n$, is not redundant, a generator b_k can only be redundant if $n+1 \le k \le m$. Furthermore since F/R^* has class at most $c + 1$, those generators b_k added for relations $[a_j, a_k] = e$ with $\mathrm{wt}(a_j) + \mathrm{wt}(a_i) > c + 1$ are trivial in F/R^* since the corresponding word $c_k = [c_j, c_i] \in P_{c+1}(F) \le R^*$. Thus we will not add new generators for these relations when performing Tietze transformations.

Now suppose that consistency checks have been performed and redundant generators have been eliminated. Then the $c_k R^*$ that correspond to the remaining generators b_k , $n+1 \le k \le n^*$ are a minimal generating set for the p-multiplicator of P . To simplify our notation we say R/R^* is generated by b_k , $n+1 \le k \le n^*$. In the next lemma we distinguish the generators of the p-multiplicator that lie in the nucleus.

LEMMA 4.10. *The nucleus* $P_c(P^*)$ *is generated by* b_j^p *and* $[b_j, b_i]$ *with* $\mathrm{wt}(b_j) = c$ *and* $\mathrm{wt}(b_i) = 1$.

Proof. By definition of the lower exponent-p-central series and the weight function, $P_c(P^*)$ contains every element of P^* that has weight $c + 1$ or higher. Since $\mathrm{wt}\left(b_j^p\right) = \mathrm{wt}\left([b_j, b_i]\right) = c + 1$, $\left\langle b_j^p, [b_j, b_i] \right\rangle \le P_c(P^*)$. Furthermore

$$P_c(P^*) = \left\langle [w, g], w^p ; \; w \in P_{c-1}(P^*), g \in P^* \right\rangle .$$

For $w \in P_{c-1}(P^*)$, $\mathrm{wt}(w) \ge c$. Thus

$$w = \prod_{k=r}^{n^*} b_k^{\gamma(k)} , \quad 0 \le \gamma(k) < p ,$$

where r is the lowest subscript of the generators of weight c in $\mathbb{P}_{n^*}$. Since b_s, $n+1 \le s \le n^*$, is central and has order p, and $[b_i, b_j] \in P_c(P^*)$, $r \le i$, $j \le n$, implies $[b_i, b_j]^p = e$, we get

$$w^p = \prod_{k=r}^{n} \left(b_k^p\right)^{\gamma(k)}$$

and

$$[w, g] = \left[\prod_{k=r}^{n} b_k^{\gamma(k)}, g\right].$$

Furthermore, since

$$g = \prod_{i=1}^{n^*} b_i^{\delta(i)}, \quad 0 \le \delta(i) < p \quad \text{and} \quad b_j, \quad r \le j \le n,$$

commute with every element of weight greater than 1,

$$[w, g] = \left[\prod_{k=r}^{n} b_k^{\gamma(k)}, \prod_{i=1}^{n^*} b_i^{\delta(i)}\right] = \prod_{k=r}^{n} \prod_{i=1}^{d} [b_k, b_i]^{\gamma(k)\delta(i)}$$

[see Huppert, 1967, Kap. III, 1.2]. Thus $P_c(P^*)$ is generated by b_j^p, $[b_j, b_i]$ with $\mathrm{wt}(b_j) = c$ and $\mathrm{wt}(b_i) = 1$. □

Now the first n generators in $\mathbb{P}_{n^*}$ for F/R^* are already ordered according to the weight function. We order the remaining generators such that the ones in the nucleus $P_c(P^*)$ are written first. Every allowable subgroup of the p-multiplicator supplements the nucleus. But every immediate descendant is a factor group of P^* by an allowable subgroup and the generators of the nucleus are given by definitions and have weight $c + 1$. Therefore the immediate descendants can be given by a consistent power commutator presentation whose generators are given by definitions and ordered according to the weight function.

To simplify our notation we will no longer distinguish between a_i in $\mathbb{P}_n$ and b_i in $\mathbb{P}_{n^*}$ as the first n generators have the same definitions.

Thus if $\mathbb{P}_n$ has the generators $a_1, \ldots, a_n$ then $\mathbb{P}_{n*}$ has the generators $a_1, \ldots, a_n, \ldots, a_{n*}$ where $a_{n+1}, \ldots, a_{n*}$ are defined as previously described.

4.3. Construction of the covering automorphism group

It follows immediately from Proposition 3.16 that every automorphism of the covering group of P that permutes allowable subgroups induces an automorphism of F/R. To complete the algorithm, we show that every automorphism α in $\mathrm{Aut}(F/R)$ can be extended to an automorphism α^* of the covering group of P such that:

(1) the action of α^* on the p-multiplicator of P is uniquely determined by α in $\mathrm{Aut}(F/R)$;

(2) those α^* in $\mathrm{Aut}(F/R^*)$ obtained as extensions of α in $\mathrm{Aut}(F/R)$ are sufficient to determine the immediate descendants of P up to isomorphism.

We only outline the theory used and omit proofs.

Again F/R is a d-generator p-group given by a consistent power commutator presentation $\mathbb{P}_n$ on n generators. We may suppose that the automorphisms in $\mathrm{Aut}(F/R)$ are given by their action on the generators $a_1, \ldots, a_d$ in $\mathbb{P}_n$.

THEOREM 4.11. *Every automorphism* α *in* $\mathrm{Aut}(F/R)$ *can be extended to an automorphism* α^* *of* F/R^* *such that* α^* *leaves* R/R^* *fixed.*

A proof of this theorem can be found in Ascione [1979, Chapter 3, p.21 *ff.*]. She proves that if α is an automorphism of F/R given by its action on the generators $a_1, \ldots, a_d$ in $\mathbb{P}_n$, then α^* defined by the same action as α on $a_1, \ldots, a_d$ but now in $\mathbb{P}_{n*}$ of F/R^* is an automorphism of F/R^* with the required properties.

DEFINITION 4.12. The subgroup of $\mathrm{Aut}(F/R^*)$ that is generated by those α^* which are extensions of $\alpha \in \mathrm{Aut}(F/R)$ is called the *covering automorphism group*, $\mathrm{Aut}^*(F/R^*)$.

COROLLARY 4.13. *Every* $\alpha^* \in \mathrm{Aut}^*(F/R^*)$ *induces a permutation on allowable subgroups in* R/R^* .

A proof can be found in Ascione [1979, Chapter 3, p. 21].

DEFINITION 4.14. The *orbit* determined by an allowable subgroup M/R^* under the permutations induced by $\mathrm{Aut}^*(F/R^*)$ is the set of images $\{(M/R^*)\alpha^* : \alpha^* \in \mathrm{Aut}^*(F/R^*)\}$.

PROPOSITION 4.15. *Two immediate descendants are isomorphic if and only if the corresponding allowable subgroups are in the same orbit under the action of* $\mathrm{Aut}^*(F/R^*)$.

Proof. Let F/M, F/N be immediate descendants of P . They are isomorphic if and only if there exists an $\alpha \in \mathrm{Aut}(F/R^*)$ with $(M/R^*)\alpha = N/R^*$, $(R/R^*)\alpha = R/R^*$ and α induces an automorphism of F/R [see proof of Proposition 3.16]. Thus F/M, F/N are isomorphic if and only if M/R^* and N/R^* are in the same orbit under the permutation induced by an automorphism in the covering automorphism group. □

Now if we choose one allowable subgroup in every orbit, called the *orbit representative*, then the corresponding factor groups of F/R^* are all immediate descendants of P determined up to isomorphism. Furthermore, every such descendant is given by a consistent power commutator presentation. To apply the algorithm to these immediate descendants it remains to construct their automorphism group.

DEFINITION 4.16. The *stabilizer* of an allowable subgroup M/R^* , $\mathrm{Stab}(M/R^*)$, is the set of automorphisms

$$\{\alpha^* : \alpha^* \in \mathrm{Aut}^*(F/R^*) \text{ with } (M/R^*)\alpha^* = M/R^*\} .$$

THEOREM 4.17. *If* F/M *is an immediate descendant of* P , *then*

$$\mathrm{Aut}(F/M) = \hat{S}.K$$

where K *is the group of automorphisms of* F/M *which induce the identity automorphism of* P *and* $\hat{S}$ *is generated by the automorphisms of* F/M *induced by* $\alpha^* \in \mathrm{Aut}^*(F/R^*)$ *with* $\alpha^* \in \mathrm{Stab}(M/R^*)$.

For a proof see Ascione [1979, Chapter 3, p. 25]. Furthermore, to arrange immediate descendants into isomorphism classes, we only need automorphisms $\alpha^* \in \mathrm{Aut}^*(F/R^*)$ that induce non-trivial permutations on the allowable subgroups. Now if $\alpha \in \mathrm{Aut}(F/R)$ is an inner automorphism then the action of the corresponding $\alpha^* \in \mathrm{Aut}^*(F/R^*)$ on R/R^* is trivial [see Ascione, 1979, Chapter 3, p. 26]. Thus inner automorphisms are not necessary for calculating orbits. Furthermore every inner automorphism α in $\mathrm{Aut}(F/R^*)$ can be extended in such a way that α^* is an inner automorphism of F/R^* . Thus inner automorphisms can be omitted from the generating set for $\mathrm{Aut}(F/R)$.

4.4. The basic steps of the algorithm

We now summarize the basic steps of the algorithm. As usual F/R is a d-generator p-group. The input for the algorithm consists of

(a) a consistent power commutator presentation $\mathbb{P}_n$ for F/R such that the generators a_i , $d+1 \le i \le n$, are given by definitions and ordered according to the weight function;

(b) a generating set for $\mathrm{Aut}(F/R)$, with inner automorphisms omitted, where every generator is given by its action on the first d generators in $\mathbb{P}_n$.

The algorithm proceeds as follows.

1. A consistent power commutator presentation $\mathbb{P}_{n^*}$ for the covering group is calculated by

1.1. adding new generators for every relation in $\mathbb{P}_n$ that is not

a definition. (Using the weight function the number of new generators added can in fact be reduced in the calculations.)

1.2. Performing consistency checks to eliminate redundant generators.

1.3. Ordering the added generators such that the ones in the nucleus are written first.

2. The covering automorphism group $\mathrm{Aut}^*(F/R^*)$ is obtained by extending the generators $\alpha_i \in \mathrm{Aut}(F/R)$ in the following way: for every $\alpha_i \in \mathrm{Aut}(F/R)$, α_i^* is defined by the same action as α_i on the first d generators of $\mathbb{P}_{n^*}$.

3. Allowable subgroups are listed [details will be given in Chapter 5].

4. The allowable subgroups are arranged into orbits under the permutations induced by $\mathrm{Aut}^*(F/R^*)$.

5. Orbit representatives are chosen from every orbit and their stabilizers are calculated.

6. Consistent power commutator presentations for the non-isomorphic immediate descendants are given.

7. The automorphism groups of these immediate descendants are obtained as described in Theorem 4.17.

CHAPTER 5

RESULTS USED IN THE ALGORITHM

In this chapter we discuss results used to simplify the calculations in the algorithm. We give a method for listing allowable subgroups of the p-multiplicator in a standardized way. For this we make use of the fact that the p-multiplicator is an elementary abelian p-group. Furthermore certain commutator identities and some properties of regular p-groups are given.

5.1. Special features of allowable subgroups

Recalling the notation of earlier chapters, $P \cong F/R$ is a d-generator p-group given by a consistent power commutator presentation $\mathbb{P}_n$, and F/R^* is the covering group given by a consistent power commutator presentation $\mathbb{P}_{n^*}$. The construction of F/R^* guarantees that the p-multiplicator R/R^* is generated by $\{a_{n+1}, \ldots, a_{n^*}\}$. Thus if we put $e = n - n^*$, the rank of R/R^*, then $R/R^* \cong A_e$, the elementary abelian p-group of rank e. Furthermore the nucleus of P is generated by $\{a_{n+1}, \ldots, a_{n+s}\}$ for some s, $n+1 \leq n+s \leq n^*$, and thus isomorphic to a subgroup N of A_e with index p^{e-s}. Thus the allowable subgroups of R/R^* are isomorphic to the subgroups of A_e that supplement N. First we give a standardized list of all subgroups of index p in A_e and then distinguish the ones that correspond to supplements of the nucleus.

LEMMA 5.1. *Let A_e be the elementary abelian p-group of rank e generated by $\{a_1, \ldots, a_e\}$. Then A_e has $\sum_{i=0}^{e-1} p^i$ subgroups of index p.*

These can be partitioned into e *classes* $S_1, \ldots, S_e$, *defined as follows:*

$$S_1 = \left\{\left\langle a_1^{\alpha(1)}a_2,\ a_1^{\alpha(2)}a_3,\ \ldots,\ a_1^{\alpha(e-1)}a_e\right\rangle : 0 \le \alpha(1), \ldots, \alpha(e-1) < p\right\}$$

$$S_2 = \left\{\left\langle a_1,\ a_2^{\alpha(1)}a_3,\ \ldots,\ a_2^{\alpha(e-2)}a_e\right\rangle : 0 \le \alpha(1), \ldots, \alpha(e-2) < p\right\}$$

$$\vdots$$

$$S_{e-1} = \left\{\left\langle a_1,\ a_2,\ \ldots,\ a_{e-1}^{\alpha(1)}a_e\right\rangle : 0 \le \alpha(1) < p\right\}$$

$$S_e = \{\langle a_1,\ a_2,\ \ldots,\ a_{e-1}\rangle\}\ .$$

Proof. A_e has $(p^e-1)/(p-1) = \sum_{i=0}^{e-1} p^i$ subgroups of index p [see Huppert, 1967, Kap. III, 8.5.b)]. Clearly all subgroups listed in $S_1, \ldots, S_e$ have index p. Since $|S_i| = p^{e-i}$,

$$\left|\bigcup_{i=1}^{e} S_i\right| \le \sum_{i=0}^{e-1} p^i\ .$$

It remains to be shown that S_i and S_j, $1 \le i, j \le e$ and $i \ne j$, are disjoint. But this is immediate: if $i \in \{2, \ldots, e\}$, then every $S \in S_i$ satisfies $a_1, \ldots, a_{i-1} \in S$ and $a_i, a_{i+1}, \ldots, a_e \notin S$, and if $i = 1$ then $a_1 \notin S$ for every $S \in S_1$ but $a_1 \in S$ for every $s \in S_i$, $2 \le i \le e$. □

DEFINITION 5.2. The subgroups of index p in A_e defined as in Lemma 5.1 are said to be given in *standard form*.

An arbitrary subgroup of index p in A_e not given in standard form can be easily brought to standard form applying the following operations:

(a) multiplying a power of a generating element by another,

(b) taking a power of a generating element.

COROLLARY 5.3. *For* $1 \le s \le e$, *let* N *be the subgroup of* A_e

generated by $\{a_1, \ldots, a_s\}$. *The set of subgroups of index* p *in* A_e *that supplement* N *is*

$$S_N = \bigcup_{i=1}^{s} S_i \quad \textit{and} \quad |S_N| = \sum_{i=e-s}^{e-1} p^i ,$$

S_i *as in Lemma* 5.1.

Proof. This follows from the property $a_1, \ldots, a_{i-1} \in S$ and $a_i, \ldots, a_e \notin S$ for every $S \in S_i$, $1 \le i \le e$. □

For practical calculations, it is convenient to use additive notation. The p-multiplicator $R/R^* = A_e$ is isomorphic to the additive group V_e^+ of a vector space V_e of dimension e over the field GF(p) with p elements. Identifying V_e with GF(p) × GF(p) × ... × GF(p) (e factors), we choose the group isomorphism $R/R^* = \langle a_{n+1}, \ldots, a_{n^*} \rangle \to V_e^+$ to satisfy $a_i \mapsto (0, \ldots, 1, \ldots, 0)$ where $(0, \ldots, 1, \ldots, 0)$ has a one in the $(i\text{-}n)$th place and zeroes in the other entries, $n+1 \le i \le n^*$. Thus if

$$\prod_{i=n+1}^{n^*} a_i^{\alpha(i)} , \quad 0 \le \alpha(i) < p ,$$

is an element of the p-multiplicator the corresponding vector, called the *exponent vector*, in V_e has the form $(\alpha(n+1), \ldots, \alpha(n^*))$. Obviously the set of allowable subgroups of R/R^* corresponds to the set of subspaces of V_e which, together with the subspace corresponding to the nucleus, generate V_e . We call these subspaces *allowable subspaces*.

Now let S be the set of subgroups listed in Corollary 5.3; then the allowable subgroups of index p^2 are subgroups of index p of a group listed in S . Thus using Corollary 5.3 and excluding duplications we get all allowable subgroups of index p^2 . Then we apply operations (a), (b) of these subgroups until the corresponding subspaces of V_e are generated

by exponent vectors that have a maximal number of zero entries on the right and a one as the entry before the first zero, or a one as the last entry if there are no zeroes on the right. Similarly the remaining allowable subgroups can be listed. We write them in additive notation and say they are given in *standard form*. It is easy to see that two such subspaces are equal if and only if the exponent vectors generating the subspaces are the same.

As the p-multiplicator is isomorphic to A_e, the covering automorphism group is isomorphic to a subgroup A of the general linear group $GL(e, p)$, since the automorphism group of A_e is isomorphic to $GL(e, p)$. Clearly two allowable subgroups are in the same orbit if and only if the corresponding allowable subspaces are mapped onto each other by a linear transformation in A.

When calculating the orbits for allowable subgroups, the following technical proposition proves to be useful.

DEFINITION 5.4. Let the p-multiplicator $R/R^* \cong A_e$, A the subgroup of $GL(e, p)$ with $A \cong \mathrm{Aut}^*(F/R^*)|_{R/R^*}$ and S a subgroup of A_e isomorphic to an allowable subgroup of R/R^*. The *orbit* determined by S under the action of A is $\{S\alpha : \alpha \in A\}$. If B is a subset of A, then the set of images $\{S\alpha : \alpha \in B\}$ is the *partial orbit* for S under B.

PROPOSITION 5.5. *Let A_e be isomorphic to the p-multiplicator R/R^*. Suppose A is defined as in Definition* 5.4 *and S a collection of isomorphic subgroups of A_e corresponding to allowable subgroups of R/R^*. Assume that the following hold:*

(1) *S can be partitioned into partial orbits O_i, $1 \le i \le r$, under the action of some subset B of A;*

(2) *there exists a subgroup $\langle a_j \rangle$, $1 \le j \le e$, such that for*

every i , $1 \le i \le r$, *there is a subgroup* $S_i \in O_i$ *with* $\langle a_j \rangle \le S_i$.

If $\alpha \in A$ *satisfies* $\langle a_j \rangle \alpha = \langle a_j \rangle$, *then* α *induces an automorphism* $\overline{\alpha}$ *of* $A_e/\langle a_j \rangle$. *Let* $\overline{A}$ *be the set of these automorphisms and* $\overline{S}$ *the set of subgroups* $S_i/\langle a_j \rangle$, $1 \le i \le r$. *Let* β *be the bijection* $O_i \mapsto S_i/\langle a_j \rangle$, $1 \le i \le r$.

Two partial orbits O_k, O_l , $1 \le k \le l \le r$ *coalesce, that is belong to the same full orbit under the action of* A , *if* $(O_k\beta)\overline{\alpha} = O_l\beta$ *for some* $\overline{\alpha} \in \overline{A}$.

Proof. Suppose $(O_k\beta)\overline{\alpha} = O_l\beta$ for some $\overline{\alpha} \in \overline{A}$. Then, for $g \in S_k$, $g\alpha + \langle a_j \rangle = (g+\langle a_j \rangle)\overline{\alpha} \in S_l/\langle a_j \rangle$, so $g\alpha \in S_l$. Thus $S_k\alpha = S_l$ and O_k, O_l belong to the same orbit.

5.2. Commutator identities for finite p-groups of a known class

For determining the images of the generators of the covering group under the action of the extended automorphisms some commutator identities are needed.

LEMMA 5.6. *Let* $[a, b]$ *be a commutator in a* p*-group of class* 2 , *then for* $n \in \mathbb{N}$,

(a) $[a^n, b] = [a, b^n] = [a, b]^n$,

(b) $(ab)^n = a^n b^n [b, a]^{\binom{n}{2}}$.

Proof. Since P has class 2 , $P_2(P) = E$. Thus every commutator $[a, b]$ lies in the centre of P . We will now prove the lemma by induction on n . If $n = 1$, *(a)* and *(b)* hold. Take $n > 1$.

(a)

$$[a^n, b] = [a, b]^{a^{n-1}}[a^{n-1}, b] \quad \text{by direct computation}$$

$$= [a, b][a^{n-1}, b] \quad \text{since } [a, b] \in Z(P)$$

$$= [a, b]^n \quad \text{by induction.}$$

Similarly $[a, b^n] = [a, b]^n$.

(b)

$$(ab)^n = (ab)^{n-1}(ab) = a^{n-1}b^{n-1}[b, a]^{\binom{n-1}{2}}ab \quad \text{by induction}$$

$$= a^{n-1}b^{n-1}ab[b, a]^{\binom{n-1}{2}} \quad \text{since } [b, a] \in Z(P)$$

$$= a^n b^{n-1}[b, a]^{n-1}b[b, a]^{\binom{n-1}{2}} \quad \text{by } (a)$$

$$= a^n b^n [b, a]^{\binom{n}{2}} \quad \text{since } [b, a]^{n-1} \in Z(P) .$$

In the following proposition we use the standard notation $[a_1, \ldots, a_n]$ for *simple commutators*. This is defined recursively by $[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$. We only state the proposition. The proof follows the same argument as the one of Lemma 5.6.

PROPOSITION 5.7. *The following equalities hold for commutators in a finite p-group.*

(a) If $\mathrm{cl}(P) = 3$, *then*

$$[a, b^n] = [a, b]^n[a, b, b]^{\binom{n}{2}} ,$$

$$[a^n, b] = [a, b]^n[a, b, a]^{\binom{n}{2}} ,$$

$$(ab)^n = a^n b^n [a, b]^{\binom{n}{2}}[a, b, b]^{\binom{n}{3}}[a, b, a]^{\binom{n}{2}+2\binom{n}{3}} .$$

(b) If $\mathrm{cl}(P) = 4$, *then*

$$[a, b^n] = [a, b]^n [a, b, b]^{\binom{n}{2}} [a, b, b, b]^{\binom{n}{3}} ,$$

$$[a^n, b] = [a, b]^n [a, b, a]^{\binom{n}{2}} [a, b, a, a]^{\binom{n}{3}} ,$$

$$(ab)^n = a^n b^n [b, a]^{\binom{n}{2}} [b, a, a]^{\binom{n}{3}} [b, a, b]^{\binom{n}{2}+2\binom{n}{3}} [b, a, a, a]^{\binom{n}{4}}$$

$$[b, a, a, b]^{\binom{n}{3}+\binom{n}{4}} [b, a, b, a]^{\binom{n}{3}+2\binom{n}{4}} [b, a, b, b]^{2\binom{n}{3}+3\binom{n}{4}} .$$

(c) If $\mathrm{cl}(P) = 5$, *then*

$$[a, b^n] = [a, b]^n [a, b, b]^{\binom{n}{2}} [a, b, b, b]^{\binom{n}{3}} [a, b, b, b, b]^{\binom{n}{4}}$$

$$[[a, b, b], [a, b]]^{\binom{n}{3}} ,$$

$$[a^n, b] = [a, b]^n [a, b, a]^{\binom{n}{2}} [a, b, a, a]^{\binom{n}{3}} [a, b, a, a, a]^{\binom{n}{4}}$$

$$[[a, b, a][a, b]]^{n^2+\binom{n}{2}+2\binom{n}{3}} . \quad \square$$

Note that we do not calculate $(ab)^n$ in general for $\mathrm{cl}(P) = 5$. This is because the only time such a product will occur in later calculations, the exponent will be p and we will be able to avoid the calculation using properties of regular p-groups. We now begin the discussion of these.

5.3. Regular p-groups

In this section we will state some results for regular p-groups which are important for our calculations.

DEFINITION 5.8. A p-group P is regular if for all elements a, b in P , $a^p b^p = (ab)^p \prod_i c_i^p$ for some c_i in $\langle a, b \rangle'$, the commutator subgroup of $\langle a, b \rangle$.

PROPOSITION 5.9. *If* P *is a* p*-group with* $|P| \leq p^p$, *then* P *is regular.*

For a proof see B. Huppert [1967, Kap. III, 10.2.b].

Since we choose $p \geq 7$, all groups with order at most p^6 will be regular.

LEMMA 5.10. *If P is a regular p-group and the commutator subgroup has exponent p, then $a^p b^p = (ab)^p$ for all elements a, b in P.*

Proof. Since P is regular $a^p b^p = (ab)^p \prod_i c_i^p$ for some c_i in $\langle a, b\rangle'$. But $\langle a, b\rangle'$ is a subgroup of the commutator subgroup of P and hence has exponent p. Thus $\prod_i c_i^p = e$.

CHAPTER 6

SIGNIFICANT CALCULATIONS OF DESCENDANTS OF $C_p \times C_p$

Our aim is the construction of all 2-generator p-groups, $p \geq 7$, of order up to p^6. By Corollary 3.4 we know that all such groups are descendants of $C_p \times C_p$. Therefore we will apply the algorithm to $C_p \times C_p$ and resulting immediate descendants and their immediate descendants, and so on, until they have order p^6. In this chapter we only describe the first step and some significant examples of the later steps in detail. The list of all descendants calculated is given in Chapter 7.

To simplify our notation we will not distinguish between allowable subgroups and corresponding allowable subspaces or automorphisms and corresponding linear transformations, since we have shown in Chapter 5 that they are essentially the same. Furthermore to shorten the presentations of the groups we will use the fact that all immediate descendants, called a *family*, of a p-group P have certain similarities. In particular

(a) all definitions in the power commutator presentation of P - *family definitions* - remain definitions for every descendant of P [see construction of the covering group in Chapter 4],

(b) all relations that are not definitions in the power commutator presentation of the covering group - *family relations* - hold in every immediate descendant.

Therefore we will first give the family definitions and relations. Then we will tabulate the definitions and relations for the added generators in the presentations of the immediate descendants. Together they give the presentations of the immediate descendants. The first two independent generators a_1, a_2 are always omitted.

6.1. Immediate descendants of $C_p \times C_p$

Let $C_p \times C_p$ be given by the consistent power commutator presentation:

$$\langle a_1, a_2; [a_2, a_1] = a_1^p = a_2^p = e \rangle .$$

The automorphism group of $C_p \times C_p$ is isomorphic to $GL(2, p)$ which can be generated by four automorphisms with the following action on the generators of $C_p \times C_p$ [see Rotman, 1965, p. 158]:

	a_1	a_2
α_1	a_1	$a_1 a_2$
α_2	$a_1 a_2$	a_2
α_3	a_1^{ε}	a_2
α_4	a_1	a_2^{ε}

ε denotes a primitive root of unity modulo p .

The covering group of $C_p \times C_p$ has the presentation:

$$\langle a_1, \ldots, a_5; a_3 = [a_2, a_1], a_4 = a_1^p, a_5 = a_2^p, a_i, 3 \le i \le 5,$$

$$\text{is central and of order } p \rangle .$$

Since $\mathrm{wt}(a_i) = 2$, $3 \le i \le 5$, the p-multiplicator and the nucleus are equal in this case. They have order p^3 . Thus they can be presented by $\langle (1, 0, 0), (0, 1, 0), (0, 0, 1) \rangle$ and the allowable subgroups can be written as follows [see Chapter 5]:

(a) index p

$\langle (\alpha, 1, 0), (\beta, 0, 1) \rangle$ with $0 \le \alpha, \beta < p$,

$\langle (1, 0, 0), (0, \gamma, 1) \rangle$ with $0 \le \gamma < p$,

$\langle (0, 1, 0), (0, 0, 1) \rangle$;

(b) index p^2

$$\langle (\alpha, \beta, 1) \rangle \text{ with } 0 \leq \alpha, \beta < p ,$$

$$\langle (\gamma, 1, 0) \rangle \text{ with } 0 \leq \gamma < p ,$$

$$\langle (1, 0, 0) \rangle ;$$

(c) index p^3

$$\langle (0, 0, 0) \rangle .$$

Now we calculate the action of the extended automorphisms α_i^* of α_i, $1 \leq i \leq 4$, on the p-multiplicator, representing them by 3×3 matrices.

$$a_3\alpha_1^* = [a_1a_2, a_1] = a_3 ,$$

$$a_4\alpha_1^* = a_4 , \qquad \text{Thus } \alpha_1^* = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} .$$

$$a_5\alpha_1^* = (a_1a_2)^p = a_1^p a_2^p a_3^{\binom{p}{2}} = a_4a_5 .$$

$$a_3\alpha_2^* = [a_2, a_1a_2] = a_3 ,$$

$$a_4\alpha_2^* = (a_1a_2)^p = a_4a_5 , \qquad \text{Thus } \alpha_2^* = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} .$$

$$a_5\alpha_2^* = a_5 .$$

$$a_3\alpha_3^* = \left[a_2, a_1^{\varepsilon}\right] = a_3^{\varepsilon} ,$$

$$a_4\alpha_3^* = \left(a_1^{\varepsilon}\right)^p = a_4^{\varepsilon} , \qquad \text{Thus } \alpha_3^* = \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

$$a_5\alpha_3^* = a_5 .$$

$$a_3\alpha_4^* = \left[a_2^{\varepsilon}, a_1\right] = a_3^{\varepsilon} ,$$

$$a_4\alpha_4^* = a_4 , \qquad \text{Thus } \alpha_4^* = \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix} .$$

$$a_5\alpha_4^* = \left(a_2^{\varepsilon}\right)^p = a_5^{\varepsilon} .$$

Under the action of α_i^*, $1 \leq i \leq 4$, the set of allowable subgroups partitions into 7 orbits:

1. $\{\langle (0, 1, 0), (0, 0, 1)\rangle\}$,

2. $\{\langle (1, 0, 0), (0, 1, 0)\rangle, \langle (1, 0, 0), (0, \alpha, 1)\rangle : 0 \leq \alpha < p\}$,

3. $\{\langle (\alpha, 1, 0), (\beta, 0, 1)\rangle : 0 \leq \alpha, \beta < p$, and not $\alpha = \beta = 0\}$,

4. $\{\langle (1, 0, 0)\rangle\}$,

5. $\{\langle (0, 1, 0)\rangle, \langle (0, \beta, 1)\rangle : 0 \leq \beta < p\}$,

6. $\{\langle (\alpha, \beta, 1)\rangle, \langle (\gamma, 1, 0)\rangle : 0 \leq \beta < p, 1 \leq \alpha, \gamma < p\}$,

7. $\{\langle 0, 0, 0\rangle\}$.

Now if we choose one orbit representative for each orbit and factor out the corresponding subgroup of the p-multiplicator, we get 7 immediate descendants. To keep the number of relations in the presentation of immediate descendants minimal, we choose orbit representatives with the largest possible number of zero entries. The immediate descendants of $C_p \times C_p$ can be presented as follows:

Let 2 denote $C_p \times C_p$. This code is chosen to indicate the number of generators. A hyphen separates immediate descendants and the first digit after it denotes the number of generators added. The digit following the number of generators indicates the number we give that particular immediate descendant when listing it. A square bracket after the last digit stands for the fact that this group has no descendants.

FAMILY 2

Name	$[a_2, a_1]$	α_1^p	α_2^p
2-11	a_3	.	.
2-12	.	a_3	.
2-13]	a_3	.	a_3
2-21	.	a_3	a_4
2-22	a_3	.	a_4
2-23	a_3	a_3	a_4
2-31	a_3	a_4	a_5

It remains to find the stabilizer of every orbit representative. This is necessary for the construction of the automorphism group of the corresponding immediate descendant. Since the orbit representatives for orbits 1, 3 and 4, are fixed under all automorphisms α_i^*, $1 \le i \le 4$, the whole covering automorphism group is their stabilizer. For the orbit representatives of 2 and 5, $\alpha_1^*, \alpha_3^*, \alpha_4^*$ generate the stabilizer. The stabilizer of the orbit representative of 6 is generated by α_1^*, α_3^*.

6.2. Immediate descendants of 2-11

For the presentation of 2-11 see the preceding section. The automorphism group of 2-11 is generated by the extensions of $\alpha_i \in \mathrm{Aut}(C_p \times C_p)$. This is because the automorphisms of 2-11 that induce the identity automorphism of $C_p \times C_p$ are $\alpha_5 : a_1 \mapsto a_1 a_3 = a_1^{a_2^{-1}}$, $a_2 \mapsto a_2$ and $\alpha_6 : a_1 \mapsto a_1$, $a_2 \mapsto a_2 a_3 = a_2^{a_1}$, and these are inner automorphisms. Thus they can be omitted from the generating set.

The covering group of 2-11 can be presented by:

$$\langle a_1, \ldots, a_7; a_3 = [a_2, a_1], a_4 = [a_3, a_1], a_5 = [a_3, a_2], a_6 = a_1^p, a_7 = a_2^p \rangle.$$

Note that we omit pth powers and commutators that are trivial.

The p-multiplicator is generated by a_i, $4 \le i \le 7$, and the nucleus is generated by a_4, a_5. Thus allowable subgroups can be listed as follows:

(a) index p :

$\langle (\alpha, 1, 0, 0), (\beta, 0, 1, 0), (\gamma, 0, 0, 1) \rangle$, $0 \le \alpha, \beta, \gamma < p$,

$\langle (1, 0, 0, 0), (0, \delta, 1, 0), (0, \eta, 0, 1) \rangle$, $0 \le \delta, \eta < p$;

(b) index p^2 :

$\langle (\alpha, \beta, 1, 0), (\gamma, \delta, 0, 1) \rangle$, $0 \le \alpha, \beta, \gamma, \delta < p$.

The action of the extended automorphisms on the p-multiplicator is now calculated.

$$a_4\alpha_1^* = [[a_1a_2, a_1], a_1] = a_4 ,$$

$$a_5\alpha_1^* = [a_3, a_1, a_2] = [a_3, a_1][a_3, a_2] = a_4a_5 ,$$

$$a_6\alpha_1^* = a_6 ,$$

$$a_7\alpha_1^* = (a_1a_2)^p = a_1^p a_2^p a_3^{\binom{p}{2}} = a_6a_7 .$$

Thus $\alpha_1^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$.

Similarly we get

$$\alpha_2^* = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \alpha_3^* = \begin{pmatrix} \varepsilon^2 & 0 & 0 & 0 \\ 0 & \varepsilon & 0 & 0 \\ 0 & 0 & \varepsilon & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \alpha_4^* = \begin{pmatrix} \varepsilon & 0 & 0 & 0 \\ 0 & \varepsilon^2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \varepsilon \end{pmatrix} .$$

We arrange the allowable subgroups of type (a) into orbits using Proposition 5.5. Applying α_1^{*x}, $0 \le x < p$, and α_2^*, we can partition them into p^2 partial orbits of length $p + 1$ in the following way:

$$\langle (0, 1, 0, 0), (\alpha, 0, 1, 0), (\beta, 0, 0, 1)\rangle\alpha_1^{*x}$$

$$= \langle (x, 1, 0, 0), (\alpha, 0, 1, 0), (\beta-\alpha x, 0, 0, 1)\rangle ,$$

$0 \le \alpha, \beta, x < p$. For every such α, β, α_1^{*x} gives a partial orbit of length p. Since

$$(1, 0, 0, 0) \notin \langle (x, 1, 0, 0), (\alpha, 0, 1, 0), (\beta-\alpha x, 0, 0, 1)\rangle ,$$

for all α, β, x, $0 \le \alpha, \beta, x < p$ and

$$\langle (1, 0, 0, 0), (0, -\beta, 1, 0), (0, \alpha-\beta, 0, 1)\rangle\alpha_2^*$$

$$= \langle (1, 1, 0, 0), (0, -\beta, 1, 1), (0, \alpha-\beta, 0, 1)\rangle$$

$$= \langle (1, 1, 0, 0), (\alpha, 0, 1, 0), (\beta-\alpha, 0, 0, 1)\rangle ,$$

we can increase the length of every partial orbit, obtained by α_1^{*x}, by one. Thus α_1^{*x}, α_2^* induce a partition of the $p^3 + p$ allowable subgroups

of type (a) into partial orbits of length $p + 1$. Furthermore there is an allowable subgroup containing $\langle (0, 1, 0, 0) \rangle$ in every partial orbit.

If we factor out $\langle a_5 \rangle$ $(\cong \langle (0, 1, 0, 0) \rangle)$ then the set $\overline{S}$ defined as in Proposition 5.5 has p^2 elements. They can be presented as follows:

$$\langle (\alpha, 1, 0), (\beta, 0, 1) \rangle , \quad 0 \leq \alpha, \beta < p .$$

The automorphism group $\overline{A}$ defined as in Proposition 5.5 can be generated by

$$\overline{\alpha}_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} , \quad \overline{\alpha}_3 = \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix} , \quad \overline{\alpha}_4 = \begin{pmatrix} \varepsilon^2 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

Now the orbits in the factor group are

1. $\{\langle (0, 1, 0), (0, 0, 1) \rangle\}$,
2. $\{\langle (\alpha, 1, 0), (0, 0, 1) \rangle : 0 \leq \alpha < p\}$,
3. $\{\langle (\alpha, 1, 0), (\beta, 0, 1) \rangle : 0 \leq \alpha < p, \beta \text{ is a square}\}$,
4. $\{\langle (\alpha, 1, 0), (\beta, 0, 1) \rangle : 0 \leq \alpha < p, \beta \text{ is a non-square}\}$.

Now the partial orbits which correspond to groups in $\overline{S}$ that lie in the same orbit coalesce. It can be shown that they are the full orbits under the action of the covering automorphism group.

Thus there are four immediate descendants of 2-11 of order p^4 which can be presented as follows:

FAMILY 2-11

family definitions: $a_3 = [a_2, a_1]$

family relations: $a_3^p = e$

Name	$[a_3, a_1]$	$[a_3, a_2]$	a_1^p	a_2^p
2-11-11	a_4	.	.	.
2-11-12]	a_4	.	a_4	.
2-11-13a] , $a = 1, \varepsilon$	a_4	.	.	a_4^a

For the calculation of the immediate descendants of order p^5 it proves to be useful to determine an upper bound for the orbit length first. Every allowable subgroup of index p^2 gives rise to such an immediate descendant. Those subgroups are presented by $\langle (\alpha, \beta, 1, 0), (\gamma, \delta, 0, 1)\rangle$, $0 \le \alpha, \beta, \gamma, \delta < p$. The presentation guarantees that two such subgroups $\langle (\alpha_1, \beta_1, 1, 0), (\gamma_1, \delta_1, 0, 1)\rangle$, $\langle (\alpha_2, \beta_2, 1, 0), (\gamma_2, \delta_2, 0, 1)\rangle$ are equal only if $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$, $\gamma_1 = \gamma_2$, $\delta_1 = \delta_2$ [see Section 5.1]. Thus we can represent $\langle (\alpha, \beta, 1, 0), (\gamma, \delta, 0, 1)\rangle$ by 2×2 matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Furthermore all images of an allowable subgroup under the action of the covering automorphism group, when written in standard form, can be represented by 2×2 matrices. It will be shown that two allowable subgroups are in the same orbit only if for the corresponding matrices M, N either $\det(M) = \det(N)$ or $\big((\mathrm{tr}(M))^2\big)/\big(\det(M)\big) = \big((\mathrm{tr}(N))^2\big)/\big(\det(N)\big)$. To do so we calculate the action of α_i^*, $1 \le i \le 4$ on the 2×2 matrices representing allowable subgroups. Let $0 \le \alpha, \beta, \gamma, \delta < p$, $0 \le a, b < p$, $1 \le c, d < p$. Then

$$\langle (\alpha, \beta, 1, 0), (\gamma, \delta, 0, 1)\rangle \alpha_1^{*a} = \langle (\alpha+\beta a, \beta, 1, 0), (\gamma+\delta a, \delta, a, 1)\rangle$$
$$= \langle (\alpha+\beta a, \beta, 1, 0), \big(\gamma+a(\delta-\alpha)-\beta a^2, \delta-\beta a, 0, 1\big)\rangle .$$

Thus we may set

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \alpha_1^{*a} = \begin{pmatrix} \alpha+\beta a & \beta \\ \gamma+a(\delta-\alpha)-\beta a^2 & \delta-\beta a \end{pmatrix} .$$

Similarly

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \alpha_2^{*b} = \begin{pmatrix} \alpha-b\gamma & \beta+b(\alpha-\delta)-\gamma b^2 \\ \gamma & \gamma b+\delta \end{pmatrix} ,$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \alpha_3^{*c} = \begin{pmatrix} \alpha\varepsilon^c & \beta \\ \gamma\varepsilon^{2c} & \delta\varepsilon^c \end{pmatrix} ,$$

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\alpha_4^{*d} = \begin{pmatrix}\alpha\varepsilon^d & \beta\varepsilon^{2d}\\ \gamma & \delta\varepsilon^d\end{pmatrix} .$$

Set $M = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$. Simple computations show that $\det(M) = 0$ implies $\det(M\alpha_i^*) = 0$, $1 \le i \le 4$, and that if $\det(M) \neq 0$, then

$$\left((\mathrm{tr}(M))^2\right)/\left(\det(M)\right) = \left(\left(\mathrm{tr}(M\alpha_i^*)\right)^2\right)/\left(\det(M\alpha_i^*)\right) , \quad 1 \le i \le 4 .$$

Then the number of matrices M with $\det(M) = 0$ or $\left((\mathrm{tr}(M))^2\right)/\left(\det(M)\right) = c$, a fixed constant, $0 \le c < p$, is an upper bound for the length of the orbits. We only state the number of matrices in every class and omit the lengthy calculations.

(a) There are $(p^2-1)(p+1) + 1$ matrices with $\det(M) = 0$.

(b) Choose $\begin{pmatrix}0 & 1\\ a & 1\end{pmatrix}$, $1 \le a < p$, as a representative for the class of matrices with $\left((\mathrm{tr}(M))^2\right)/\left(\det(M)\right) = -(1/a) = c$. The number of matrices in each class depends on whether $1 + 4a$ is a square, a non-square or zero. If $1 + 4a$ is a square we get $(p-3)/2$ classes each containing $p(p^2-1)$ matrices. For $1 + 4a$ a non-square we get $(p-1)/2$ classes with $p(p-1)^2$ matrices in each class. In the case $1 + 4a = 0$ the number of matrices is $p^2(p-1)$.

(c) For $\left((\mathrm{tr}(M))^2\right)/\left(\det(M)\right) = 0$ we get $p^2(p-1)$ matrices.

Now we calculate the orbits.

(a) For calculating the orbits of allowable subgroups corresponding to matrices M with $\det(M) = 0$ we make use of Proposition 5.5. The subgroup factored out is $\langle a_7 \rangle$ and the automorphisms used to induce the partition into partial orbits are α_1^{*x} , $0 \le x < p$, α_2^* . We omit the actual

computations since they are very similar to the ones used for determining the immediate descendants of 2-11 of order p^4. There are four immediate descendants in this case: 2-21, 2-22, 2-23a, $a = 1, \varepsilon$. For their presentations see Chapter 7.

(b) For each a with $1 + 4a$ a square, the orbit determined by the allowable subgroup $\langle (0, 1, 0, 0), (a, 1, 0, 0) \rangle$ has at most length $p(p^2-1)$. We now show that this is exactly the orbit length.

$$\begin{pmatrix} 0 & 1 \\ a & 1 \end{pmatrix} \alpha_3^{*b} \alpha_1^{*x} = \begin{pmatrix} x & 1 \\ a\varepsilon^{2b} + x\varepsilon^b - x^2 & \varepsilon^b \end{pmatrix}, \quad 1 \le b < p, \quad 0 \le x < p.$$

Now set $\varepsilon^b = \sigma$. Then $a\sigma^2 + x\sigma - x^2 = \frac{1}{4}\sigma^2(1+4a) - (x-\frac{1}{2}\sigma)^2$. Since $1 + 4a$ is a square, the right hand side is the difference of two squares. Thus if we set $r = \frac{1}{4}\sigma^2(1+4a) - (x-\frac{1}{2}\sigma)^2$, then r takes p values. This is because every element of $GF(p)$ can be written as the difference of two squares.

Now

$$\begin{pmatrix} x & 1 \\ r & \sigma - x \end{pmatrix} \alpha_4^{*c} = \begin{pmatrix} x\varepsilon^c & \varepsilon^{2c} \\ r & (\sigma - x)\varepsilon^c \end{pmatrix}, \quad 1 \le c < p.$$

Setting $\varepsilon^c = \tau$ and applying α_2^y, $0 \le y < p$, we get

$$\begin{pmatrix} x\tau - yr & \tau^2 + y(2x\tau - \sigma\tau) + y^2 r \\ r & \sigma\tau - x\tau + yr \end{pmatrix}.$$

For $r \neq 0$ we get $p(p-1)^2$ different matrices and for $r = 0$ there are $2p(p-1)$ further matrices. Thus since we have $(p-3)/2$ choices for a, we get $(p-3)/2$ orbits of length $p(p^2-1)$.

In a similar way we can show that if $1 + 4a$ is a non-square then the length of each orbit is $p(p-1)^2$.

If $1 + 4a = 0$ then $c = 4$. We choose

$$\begin{pmatrix} 0 & 1 \\ -\frac{1}{4} & 1 \end{pmatrix}, \begin{pmatrix} 0 & \varepsilon \\ -\frac{1}{4}\varepsilon & \varepsilon \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

as representative matrices. The corresponding allowable subgroups determine three orbits of length $\left((p^2-1)(p-1)\right)/2$, $\left((p^2-1)(p-1)\right)/2$, $p-1$ respectively.

(c) For the case $\mathrm{tr}(M) = 0$, $\det(M) \neq 0$, we get two orbits of length $p\left((p-1)^2/2\right)$ and $p\left((p^2-1)/2\right)$. The representative for the first orbit is $\begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$ and for the second $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

6.3. Descendants of $C_{p^2} \times C_p$

For $C_{p^2} \times C_p$, or 2-12 in our notation, we will prove by induction on the class that its descendants of class n have the following form:

(a) $C_{p^n} \times C_p$,

(b) $\left\langle a_1, \ldots, a_n;\ a_1^{p^n} = a_2^p = e,\ [a_2, a_1] = a_1^{p^{n-1}} \right\rangle$.

Furthermore, we claim that $\mathrm{Aut}\left(C_{p^n} \times C_p\right)$ is generated by the following automorphisms:

	a_1	a_2	
α_1	a_1	a_2^{ε}	ε denotes a primitive root of unity
α_2	a_1^{ε}	a_2	modulo p
α_3	$a_1 a_2$	a_2	
α_{i+3}	$a_1 a_1^{p^i}$	a_2	$1 \leq i \leq n-1$
α_{n+3}	a_1	$a_2 a_1^{p^{n-1}}$	

Moreover it can be easily seen that the group presented in (b) has no descendants.

Simple calculations show that the descendants of $C_{p^2} \times C_p$ are as required. Thus we have to show that the immediate descendants of $C_{p^{n-1}} \times C_p$ have the desired form.

Suppose $C_{p^{n-1}} \times C_p$ is given by the consistent power commutator presentation:

$$\langle a_1, \ldots, a_n; a_1^p = a_3, a_i^p = a_{i+1}, 3 \leq i \leq n-1 \rangle .$$

Furthermore suppose the automorphism group of $C_{p^{n-1}} \times C_p$ is given as follows:

	a_1	a_2	
α_1	a_1	a_2^{ε}	
α_2	a_1^{ε}	a_2	ε denotes a primitive root of unity modulo p
α_{i+1}	$a_1 a_i$	a_2	$2 \leq i \leq n$
α_{n+2}	a_1	$a_2 a_n$	

The covering group of $C_{p^{n-1}} \times C_p$ can be presented as follows:

$$\langle a_1, \ldots, a_n, \ldots, a_{n+3}; a_3 = a_1^p, a_{i+1} = a_i^p, a_{n+2} = [a_2, a_1], a_{n+3} = a_2^p, 3 \leq i \leq n \rangle .$$

Note that generators added for $[a_i, a_1]$, $[a_i, a_2]$, $3 \leq i \leq n$, are trivial since $[a_i, a_1] = \left[a_1^{p^{i-2}}, a_1\right] = e$ and collecting $a_2 a_1^{p^{i-2}}$ in two different ways gives: $a_2 a_1^{p^{i-2}} = a_2 a_i$,

$$a_2 a_1^{p^{i-2}} = a_1^{p^{i-2}} a_2 [a_2, a_1]^{p^{i-2}} = a_i a_2 = a_2 a_i [a_i, a_2] .$$

Thus the p-multiplicator is generated by a_{n+1}, a_{n+2}, a_{n+3}. Since $\mathrm{wt}(a_{n+2})$ and $\mathrm{wt}(a_{n+3})$ are less than n and $\mathrm{wt}(a_{n+1}) = n$, the nucleus is generated by a_{n+1}. Therefore the p-multiplicator has p^2 allowable subgroups, which can be written as follows: $\langle (\alpha, 1, 0), (\beta, 0, 1) \rangle$, $0 \le \alpha, \beta < p$.

Now we determine the action of $\mathrm{Aut}^*(C_{p^{n-1}} \times C_p)$ on the p-multiplicator. Firstly the extensions of α_{i+1}, $2 \le i \le n$, act trivially on the p-multiplicator since

$$a_{n+1}\alpha_{i+1}^* = \left(a_1^{p^{n-1}}\right)\alpha_{i+1}^* = (a_1 a_i)^{p^{n-1}} = a_1^{p^{n-1}} a_i^{p^{n-1}} [a_i, a_1]^{\binom{p^{n-1}}{2}} = a_{n+1} ,$$

$$a_{n+2}\alpha_{i+1}^* = [a_2, a_1]\alpha_{i+1}^* = [a_2, a_1 a_i] = [a_2, a_i][a_2, a_1]^{a_i} = a_{n+1} ,$$

$$a_{n+3}\alpha_{i+1}^* = a_{n+3} .$$

Direct computation gives the following matrices for the action of α_1^*, α_2^*, α_{n+2}^*:

$$\alpha_1^* = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon \end{pmatrix} , \quad \alpha_2^* = \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & 1 \end{pmatrix} , \quad \alpha_{n+2}^* = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} .$$

Thus $\langle (0,1,0), (0,0,1) \rangle \alpha_{n+2}^{*a} = \langle (0,1,0), (a,0,1) \rangle$, $0 \le a < p$, and

$\langle (-1,1,0), (0,0,1) \rangle \alpha_{n+2}^{*a} \alpha_1^{*y} = \langle (-\varepsilon^{-y}, 1, 0), (a\varepsilon^{-y}, 0, 1) \rangle$, $0 \le a < p$, $1 \le y < p$, give two orbits of length p, $p^2 - p$, respectively.

Choosing $\langle (0,1,0), (0,0,1) \rangle$ and $\langle (-1,1,0), (0,0,1) \rangle$ as orbit representatives, the corresponding factor groups of the covering group of $C_{p^{n-1}} \times C_p$ have the required form. Furthermore the stabilizer of $\langle (0,1,0), (0,0,1) \rangle$

is generated by α_i^* , $1 \le i \le n+1$ and the automorphisms of $C_{p^n} \times C_p$ that induce the identity for $C_{p^{n-1}} \times C_p$ are $\alpha : a_1 \mapsto a_1 a_{n+1}$, $a_2 \mapsto a_2$ and $\beta : a_1 \mapsto a_1$, $a_2 \mapsto a_2 a_{n+1}$. Thus the automorphism group of $C_{p^n} \times C_p$ has the required form.

6.4. Immediate descendants of 2-22-16a

The groups 2-22-16a , $a = 1, \varepsilon$, each have $(p-1)/2$ immediate descendants that are not included in the list given by James [1969]. Therefore we discuss these cases in more detail. The groups can be presented by

$$\langle a_1, \ldots, a_5; a_3 = [a_2, a_1], a_4 = a_2^p, a_5 = [a_3, a_2], a_5^a = a_1^p \rangle .$$

Since the calculations for $a = \varepsilon$ are the same as for $a = 1$ we will only discuss the latter.

The automorphism group is generated by

	a_1	a_2
α_1	$a_1 a_5$	a_2
α_2	$a_1 a_4$	a_2
α_3	a_1	$a_2 a_4$
α_4	a_1	$a_1 a_2$
α_5	a_1^{ε}	a_2
α_6	a_1	a_2^{-1}

For the presentation of the covering group the following generators are added: $a_6 = [a_5, a_2]$, $a_7 = [a_3, a_1]$, $a_8 = a_4^p$, $a_9 = a_5^{-1} a_1^p$. The

non-trivial relations added are: $a_3^p = [a_4, a_1] = a_6^{-1}$. Thus the p-multiplicator has order p^4 and the nucleus has order p . The allowable subgroups can be represented by

$$\langle (\alpha, 1, 0, 0), (\beta, 0, 1, 0), (\gamma, 0, 0, 1) \rangle \ , \quad 0 \le \alpha, \beta, \gamma < p \ .$$

Calculating the covering automorphism group, one can easily see that the actions of $\alpha_1^*, \alpha_3^*, \alpha_4^*$ on the p-multiplicator are trivial and that the remaining extended automorphisms can be represented as follows:

$$\alpha_2^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \alpha_5^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix},$$

$$\alpha_6^* = \begin{pmatrix} \varepsilon & 0 & 0 & 0 \\ 0 & \varepsilon^2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \varepsilon \end{pmatrix}, \quad \alpha_7^* = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix}.$$

Now we calculate the orbits:

$$\langle (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1) \rangle \ ,$$

$$\langle (0, 1, 0, 0), (0, 0, 1, 0), (2, 0, 0, 1) \rangle$$

are mapped onto each other by α_7^* , which has order 2 , and fixed under all the other automorphisms. Thus they give an orbit of length 2 . Now the immediate descendant, obtained by factoring out

$$\langle (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1) \rangle \ (\cong \langle a_7, a_8, a_9 \rangle) \ ,$$

is isomorphic to the following group in James's list:

$$\Phi_{25}(222) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4 : [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_3, \alpha] = \alpha_4,$$

$$\alpha^{p^2} = \alpha_4, \alpha_i^{(p)} = \alpha_{i+2}, \alpha_{i+2}^p = 1 \ (i = 1, 2) \Big\rangle$$

[see James, 1969, p. A29, or p. 75 in the corrected list]. According to

James's list this group represents an isomorphism class containing p groups. However the isomorphisms he uses [see James, 1969, p. 172, or p. 41 in the corrected list] can be shown to give only two groups. The remaining $p - 2$ groups can be arranged into orbits as follows:

$$\langle (0, 1, 0, 0), (0, 0, 1, 0), (1, 0, 0, 1) \rangle$$

is fixed under all automorphisms and

$$\langle (0, 1, 0, 0), (0, 0, 1, 0), (\alpha, 0, 0, 1) \rangle \ , \quad 2 \leq \alpha < p \ ,$$

splits up into orbits of length 2 . Thus the immediate descendants missing in James's list can be presented as follows:

$$\Big\langle a_1, \ldots, a_6; a_3 = [a_2, a_1], a_4 = a_2^p, a_5 = [a_3, a_2], a_6 = [a_5, a_2],$$

$$a_1^p = a_5 a_6^y \Big\rangle \ , \quad (p-3)/2 \leq y < p \quad \text{or} \quad y = -1 \ .$$

For the other immediate descendants of 2-22-16a , $a = 1$, see Chapter 7.

CHAPTER 7

LIST OF ALL 2-GENERATOR p-GROUPS OF ORDER UP TO p^6 , $p \geq 7$

Before giving the actual list we first explain how to read it. Every group listed has a sequence of immediate descendants associated with it. In particular, this sequence starts, not counting the identity, with $A_2 = C_p \times C_p$. Every immediate descendant of a group P with class c and order p^n is a factor group of the covering group of P with class $c + 1$ and order p^{n+s} , s a natural number greater than one. Thus the class of the immediate descendants is $c + 1$ and their order is p^{n+r} , $1 \leq r \leq s$. We include this information in a graphical representation and also in the code chosen when naming the groups.

In the graphs given for the groups, every vertex denotes a group. Adjacent vertices stand for a family of immediate descendants. To distinguish between different increases in order (that is, different r) we choose different lengths for the edges. The number of immediate descendants of a group is also indicated in the graph by $[\alpha]$, α an integer.

When listing the groups we introduce the following code: $C_p \times C_p$: = 2 which indicates that the number of generators is 2 . Then immediate descendants are separated by hyphens. The first digit after the hyphen denotes the number of generators added, which is equal to r as defined above. The following digits give the number we choose for each immediate descendant when listing it. Thus the class and order can be read from the code for every group. For an example, 2-11-21 is a group of class 3 and order p^5 . When presenting the groups we simplify this as described in

the beginning of Chapter 6. Note that every added generator is central of order p, and we omit these relations from the family relations. Since we list the groups according to their orders the families have to be split up. Thus a family can be separated into several parts according to the order of the immediate descendants contained in it. We order the groups in the list in the order they occur when putting horizontal lines through the graph. For comparison purposes, we also give the names of the groups according to James's corrected list [unpublished].

Furthermore, we introduce the following letters for the cases when the number of groups depends on p :

$$a = 1, \varepsilon ,$$

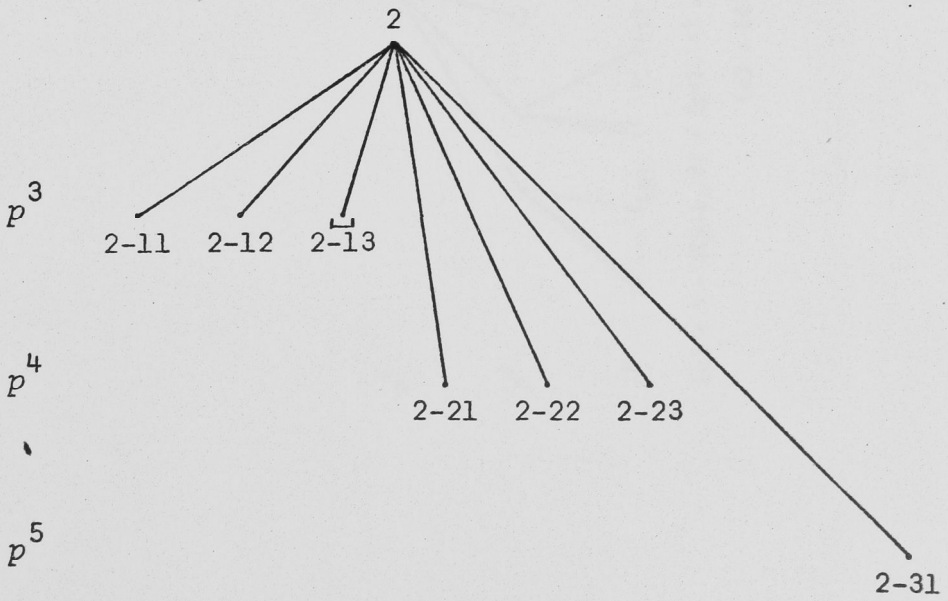
$$b = \varepsilon^{\alpha} , \quad 0 \le \alpha < (p\text{-}1, 3) ,$$

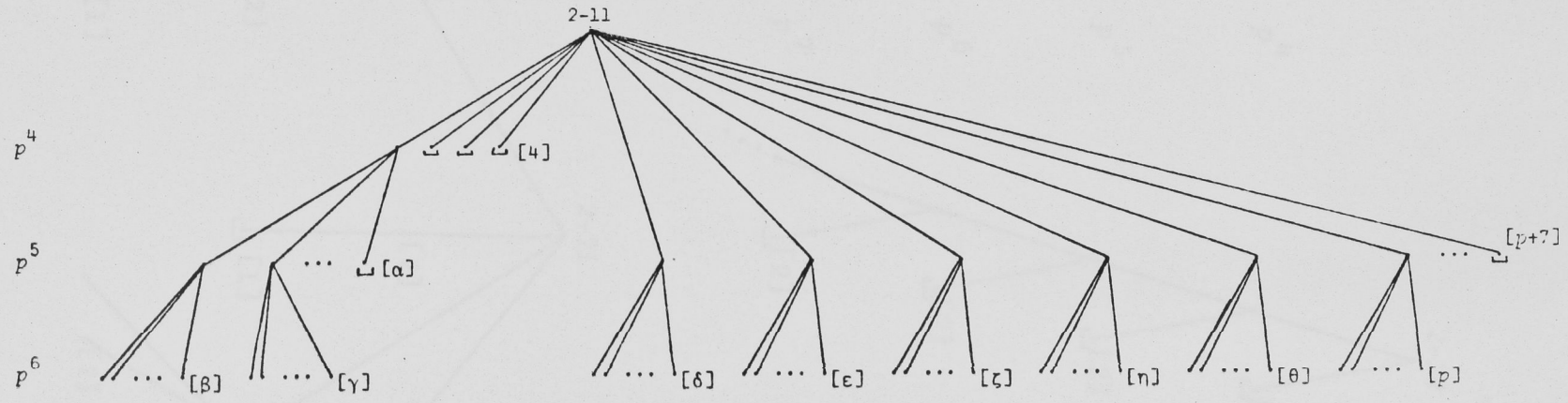
$$c = \varepsilon^{\beta} , \quad 0 \le \beta < (p\text{-}1, 4) ,$$

$$d = \varepsilon^{\gamma} , \quad 0 \le \gamma < (p\text{-}1, 5) ,$$

$$e = \varepsilon^{\delta} , \quad 0 \le \delta < (p\text{-}1, 6) ,$$

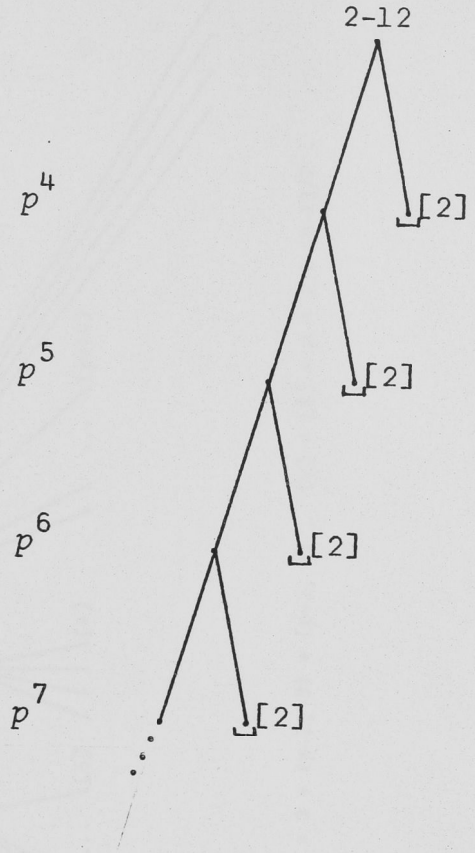
x has the range $1 \le x < p$.

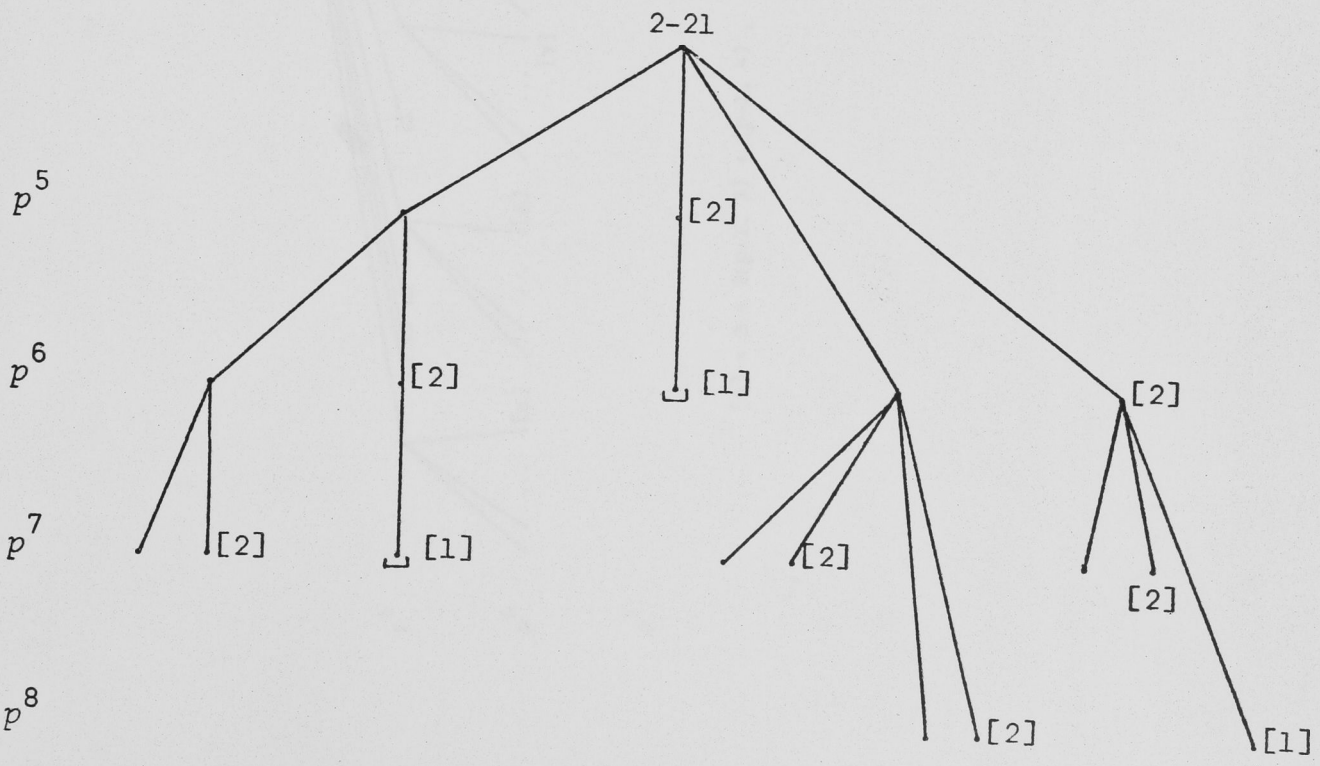


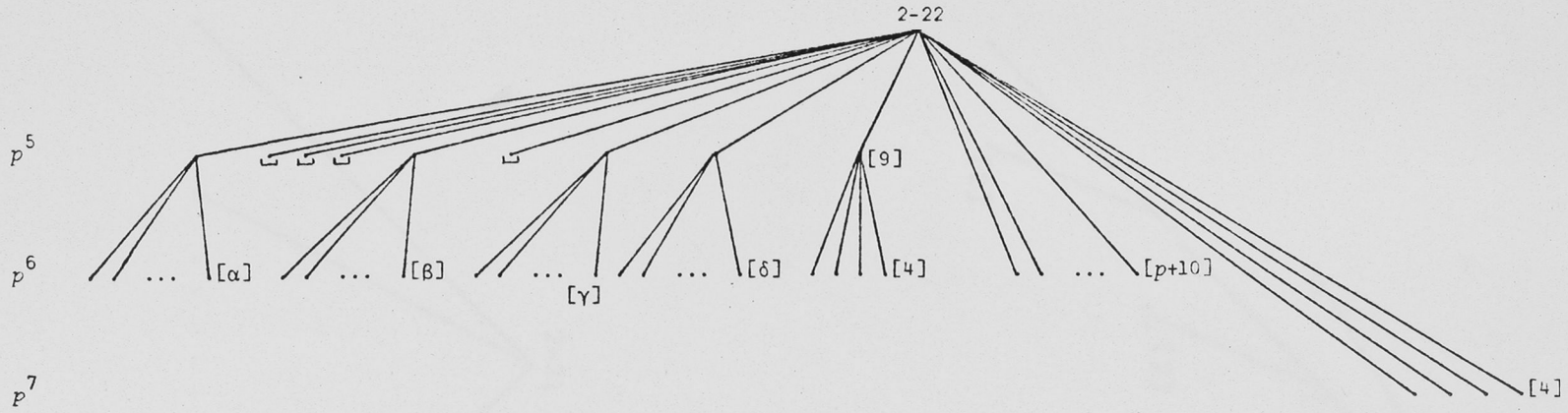


$[\alpha] = 3 + 2(p\text{-}1, 3) + (p\text{-}1, 4)$, $[\beta] = 7 + 3(p\text{-}1, 4) + (p\text{-}1, 6)$, $[\gamma] = 2p + (p\text{-}1, 4) + 2(p\text{-}1, 5) + (p\text{-}1, 6)$, $[\delta] = 5 + 3(p\text{-}1, 3)$,

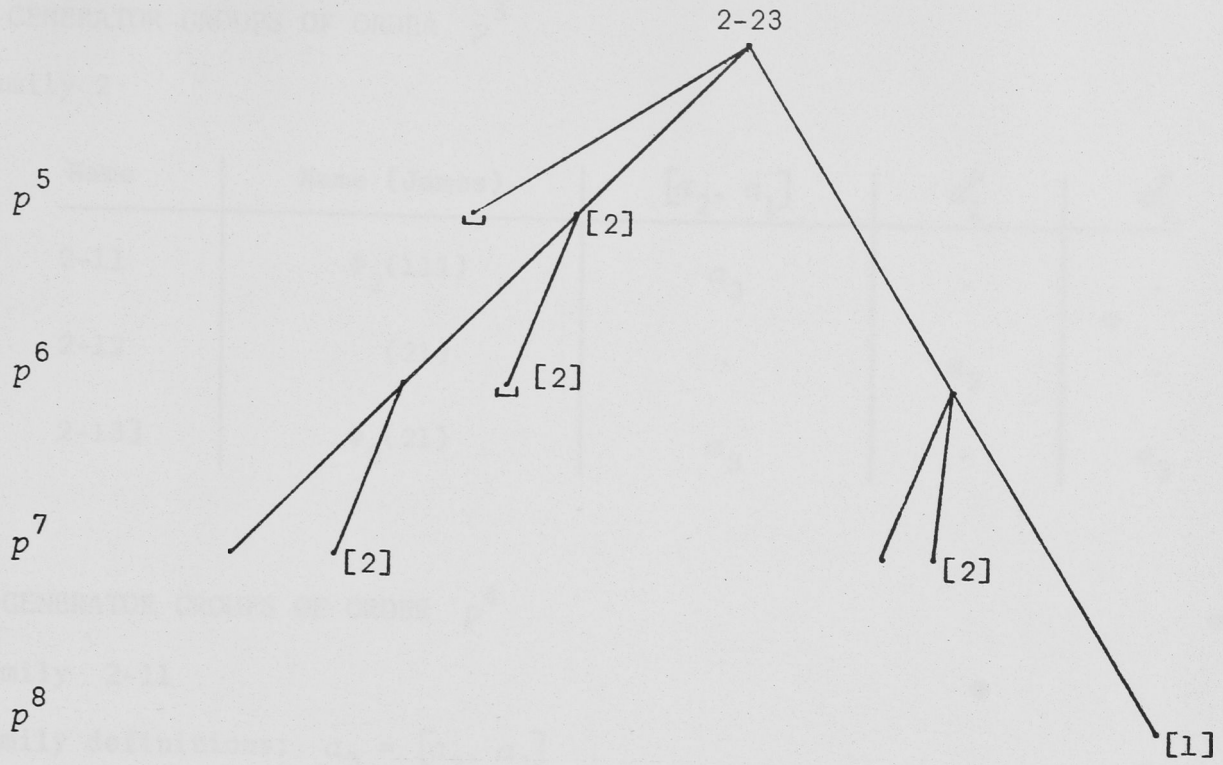
$[\varepsilon] = [\zeta] = 2 + (p\text{-}1, 3)$ (+1 if $p = 4n+1$) , $[\eta] = p + 1 + (p\text{-}1, 3)$, $[\theta] = p + 1$.

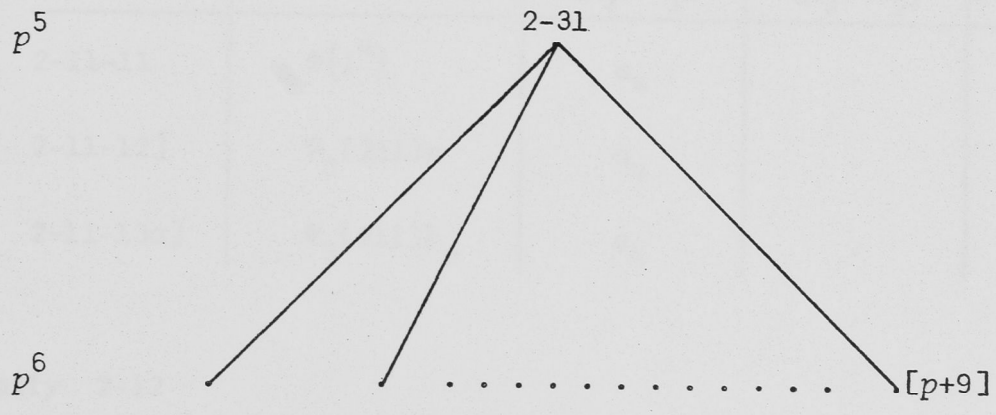

2-12
p^4
p^5
p^6
p^7
[2]
[2]
[2]
[2]


2-21
p^5
p^6
p^7
p^8
[2]
[2]
[1]
[2]
[2]
[2]
[2]
[2]
[1]



$[\alpha] = 3 + 2(p\text{-}1, 3) + (p\text{-}1, 4)$, $[\beta] = 3 + (p\text{-}1, 3) + (p\text{-}1, 4)$, $[\gamma] = [\delta] = p + 2 + (p\text{-}1)/2$.


2-23
p^5
p^6
p^7
p^8
[2]
[2]
[2]
[2]
[1]


2-31
p^5
p^6
[p+9]

2-GENERATOR GROUPS OF ORDER p^3

Family 2

Name	Name (James)	$[a_2, a_1]$	a_1^p	a_2^p
2-11	$\Phi_2(111)$	a_3	.	.
2-12	(21)	.	a_3	.
2-13]	$\Phi_2(21)$	a_3	.	a_3

2-GENERATOR GROUPS OF ORDER p^4

Family 2-11

Family definitions: $a_3 = [a_2, a_1]$

Family relations: $a_3^p = e$

Name	Name (James)	$[a_3, a_1]$	$[a_3, a_2]$	a_1^p	a_2^p
2-11-11	$\Phi(1^4)$	a_4	.	.	.
2-11-12]	$\Phi_3(211)a$	a_4	.	a_4	.
2-11-13a]	$\Phi_3(211)b_r$	a_4	.	.	a_4^a

Family 2-12

Family definitions: $a_3 = a_1^p$

Family relations: $[a_3, a_i] = e$, $i = 1, 2$

Name	Name (James)	a_3^p	$[a_2, a_1]$	a_2^p
2-12-11	(31)	a_4	.	.
2-12-12]	$\Phi_2(31)$	a_4	a_4	.

Family 2

Name	Name (James)	$[a_2, a_1]$	a_1^p	a_2^p
2-21	(22)	.	a_3	a_4
2-22	$\Phi_2(211)c$	a_3	.	a_4
2-23	$\Phi_2(22)$	a_3	a_3	a_4

2-GENERATOR GROUPS OF ORDER p^5

Family 2-11-11

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = [a_3, a_1]$

Family relations: $[a_4, a_2] = a_3^p = a_4^p = e$

Name	Name (James)	$[a_4, a_1]$	$[a_3, a_2]$	a_1^p	a_2^p
2-11-11-11	$\Phi_9(1^5)$	a_5	.	.	.
2-11-11-12	$\Phi_{10}(1^5)$	a_5	a_5	.	.
2-11-11-13]	$\Phi_9(2111)a$	a_5	.	a_5	.
2-11-11-14c]	$\Phi_{10}(2111)a_r$	a_5	a_5^c	a_5	.
2-11-11-15b]	$\Phi_9(2111)b_r$	a_5	.	.	a_5^b
2-11-11-16b]	$\Phi_{10}(2111)b_r$	a_5	a_5	.	a_5^b

Family 2-11

Family definitions: $a_3 = [a_2, a_1]$

Family relations: $a_3^p = e$

Name	Name (James)	$[a_3, a_1]$	$[a_3, a_2]$	a_1^p	a_2^p
2-11-21	$\Phi_6(1^5)$	a_4	a_5	.	.
2-11-22a	$\Phi_6(2111)b_r$	a_4	a_5	a_5^a	.

Family 2-11 (continued)

Name	Name (James)	$[a_3, a_1]$	$[a_3, a_2]$	a_1^p	a_2^p
2-11-23	$\Phi_6(2111)a$	a_4	a_5	a_4	.
2-11-24	$\Phi_6(221)b_{\frac{1}{2}(p-1)}$	a_4	a_5	a_4	a_5^{-1}
2-11-25	$\Phi_6(221)d_0$	a_4	a_5	a_5^{-1}	$a_4^{-\varepsilon}$
2-11-26]	$\Phi_6(221)c_1$	a_4	a_5	a_4	a_5
2-11-27a]	$\Phi_6(221)c_\gamma$	a_4	a_5	a_5^{-a}	$a_4^{\frac{1}{4}a}a_5^{-a}$
2-11-28x]	$\Phi_6(221)d_r$, $\Phi_6(221)b_r$	a_4	a_5	a_5^{-1}	$a_4^{x}a_5^{-1}$
($x \neq \frac{1}{4}$)	$(b_r \neq b_{\frac{1}{2}(p-1)})$				

Family 2-12-11

Family definitions: $a_3 = a_1^p$, $a_4 = a_3^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = e$, $i = 3, 4$

Name	Name (James)	a_4^p	$[a_2, a_1]$	a_2^p
2-12-11-11	(41)	a_5	.	.
2-12-11-12]	$\Phi_2(41)$	a_5	a_5	.

Family 2-21

Family definitions: $a_3 = a_1^p$, $a_4 = a_2^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = e$, $i = 3, 4$

Name	Name (James)	a_3^p	a_4^p	$[a_2, a_1]$
2-21-11	(32)	a_5	.	.
2-21-12	$\Phi_2(32)$	.	a_5	a_5

Family 2-22

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = a_3^p = a_5^p = e$, $i = 3, 4$

Name	Name (James)	$[a_3, a_1]$	$[a_3, a_2]$	a_4^p	a_1^p
2-22-11	$\Phi_3(2111)e$	a_5	.	.	.
2-22-12]	$\Phi_3(221)a$	a_5	.	.	a_5
2-22-13a]	$\Phi_3(311)b_r$	a_5	.	a_5^a	.
2-22-14	$\Phi_3(2111)d$	.	a_5	.	.
2-22-15]	$\Phi_3(311)a$	.	a_5	a_5	.
2-22-16a	$\Phi_3(221)b_r$	.	a_5	.	a_5^a
2-22-17	$\Phi_2(311)c$	.	.	a_5	.

Family 2-23

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$

Family relations; $[a_3, a_1] = [a_4, a_2] = e$, $[a_3, a_2]^{-1} = [a_4, a_1] = a_3^p$

Name	Name (James)	$[a_3, a_2]$	a_4^p	a_1^p
2-23-11]	$\Phi_8(32)$	a_5	.	a_3
2-23-12	$\Phi_2(32)a_2$	.	a_5	a_3

Family 2

Name	Name (James)	$[a_2, a_1]$	a_1^p	a_2^p
2-31	$\Phi_2(221)d$	a_3	a_4	a_5

GROUPS OF ORDER p^6

Family 2-11-11-11

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = [a_3, a_1]$, $a_5 = [a_4, a_1]$

Family relations: $a_i^p = e$, $3 \le i \le 5$, $[a_4, a_2] = [a_4, a_3]^{-1} = [a_5, a_2]$

Name	Name (James)	$[a_5, a_1]$	$[a_5, a_2]$	$[a_3, a_2]$	a_1^p	a_2^p
2-11-11-11-11	$\Phi_{35}(1^6)$	a_6	.	.	.	.
2-11-11-11-12	$\Phi_{37}(1^6)$	.	a_6	.	.	.
2-11-11-11-13	$\Phi_{36}(1^6)$	a_6	.	a_6	.	.
2-11-11-11-14	$\Phi_{35}(21^4)a$	a_6	.	.	a_6	.
2-11-11-11-15a	$\Phi_{37}(21^4)a_r$	.	a_6	.	a_6^a	.
2-11-11-11-16e	$\Phi_{36}(21^4)a_r$	a_6	.	a_6	a_6^e	.
2-11-11-11-17c	$\Phi_{35}(21^4)b_r$	a_6	.	.	.	a_6^c
2-11-11-11-18	$\Phi_{37}(21^4)b_p$	.	a_6	.	.	a_6
2-11-11-11-19c	$\Phi_{36}(21^4)b_r$	a_6	.	a_6	.	a_6^c
2-11-11-11-110c	$\Phi_{37}(21^4)b_r$	.	a_6	.	a_6^c	a_6

Family 2-11-11-12

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = [a_3, a_1]$, $a_5 = [a_4, a_1]$

Family relations: $a_i^p = e$, $3 \le i \le 5$, $[a_5, a_2] = [a_4, a_3]^{-1}$

$= [a_4, a_2][a_5, a_1]^{-1}$

Name	Name (James)	$[a_5, a_1]$	$[a_5, a_2]$	$[a_3, a_2]$	a_1^p	a_2^p
2-11-11-12-11	$\Phi_{38}(1^6)$	a_6	.	a_5	.	.
2-11-11-12-12	$\Phi_{39}(1^6)$	a_6	a_6	a_5	.	.
2-11-11-12-13c	$\Phi_{38}(21^4)b_{p+r}$	a_6	.	a_5	.	a_6^c
2-11-11-12-14d	$\Phi_{38}(21^4)a_r$	a_6	.	a_5	a_6^d	.
2-11-11-12-15x	$\Phi_{38}(21^4)b_r$	a_6	.	a_5	a_6^x	a_6^x
2-11-11-12-16e	$\Phi_{39}(21^4)a_r$	.	a_6	a_5	a_6^e	.
2-11-11-12-17d	$\Phi_{39}(21^4)b_{p+r}$	.	a_6	a_5	.	a_6^d
2-11-11-12-18x	$\Phi_{39}(21^4)b_r$	.	a_6	a_5	a_6^x	a_6^x

Family 2-11-21

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = [a_3, a_1]$, $a_5 = [a_3, a_2]$

Family relations: $[a_4, a_2] = [a_5, a_1]$, $a_i^p = e$, $3 \le i \le 5$

Name	Name (James)	$[a_4, a_1]$	$[a_4, a_2]$	$[a_5, a_2]$	a_1^p	a_2^p
2-11-21-11	$\Phi_{23}(1^6)$	a_6	.	.	.	.
2-11-21-12	$\Phi_{40}(1^6)$	a_6	a_6	.	.	.
2-11-21-13	$\Phi_{41}(1^6)$	a_6	.	$a_6^{-\varepsilon}$	.	.
2-11-21-14b	$\Phi_{23}(21^4)c_r$	a_6	.	.	.	a_6^b
2-11-21-15	$\Phi_{23}(21^4)a$	a_6	.	.	a_6	.

Family 2-11-21 (continued)

Name	Name (James)	$[a_4, a_1]$	$[a_4, a_2]$	$[a_5, a_2]$	a_1^p	a_2^p
2-11-21-16*b*	$\Phi_{41}(21^4)a_r$	a_6	.	$a_6^{-\varepsilon}$	a_6^b	.
2-11-21-17	$\Phi_{40}(21^4)a_p$	.	a_6	.	a_6	.
2-11-21-18*b*	$\Phi_{40}(21^4)a_r$	.	a_6	.	a_6^b	a_6

Family 2-11-22*a*

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = [a_3, a_1]$, $a_5 = [a_3, a_2]$

Family relations: $[a_4, a_2] = [a_5, a_1] = [a_5, a_2] = a_i^p = e$, $3 \le i \le 5$

Name	Name (James)	$[a_4, a_1]$	a_1^p	a_2^p
2-11-22*a*-11	$\Phi_{23}(21^4)b$	a_6	a_5^a	.
2-11-22*a*-12	$\Phi_{23}(21^4)b_{1,1}$	a_6	$a_5^a a_6$	.
2-11-22*a*-13*	$\Phi_{23}(21^4)b_{\gamma,1}$	a_6	$a_5^a a_6^\varepsilon$	.
2-11-22*a*-14*b*	$\Phi_{29}(2211)c_{r,s}$	a_6	a_5^a	a_6^b

* only if $p = 4n + 1$.

Family 2-11-23

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = [a_3, a_1]$, $a_5 = [a_3, a_2]$

Family relations: $[a_5, a_1] = [a_4, a_1] = [a_4, a_2] = a_i^p = e$, $3 \le i \le 5$

Name	Name (James)	$[a_5, a_2]$	a_1^p	a_2^p
2-11-23-11	$\Phi_{23}(21^4)d$	a_6	a_4	.
2-11-23-12*b*	$\Phi_{23}(21^4)e_r$	a_6	$a_4 a_6^b$	.
2-11-23-13	$\Phi_{23}(2211)a$	a_6	a_4	a_6
2-11-23-14*x*	$\Phi_{23}(2211)b_r$	a_6	$a_4 a_6^x$	a_6

Family 2-11-24

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = [a_3, a_1]$, $a_5 = [a_3, a_2]$

Family relations: $[a_5, a_2] = [a_4, a_1] = a_i^p = e$, $i = 4, 5$,

$$[a_5, a_1]^{-1} = [a_4, a_2]^{-1} = a_3^p$$

Name	Name (James)	$[a_4, a_2]$	a_1^p	a_2^p
2-11-24-11	$\Phi_{42}(222)a_6$	a_6	$a_4 a_6^{-\frac{1}{2}}$	$a_5^{-1} a_6^{\frac{1}{2}}$
2-11-24-12	$\Phi_{42}(222)a$	a_6	$a_4 a_6^{-\frac{1}{2}}$	$a_5^{-1} a_6^{-\frac{1}{2}}$
2-11-24-13x	$\Phi_{42}(222)a_r$ $(r \neq 0)$	a_6	$a_4 a_6^{x-\frac{1}{2}}$	$a_5^{-1} a_6^{-\frac{1}{2}}$

Family 2-11-25

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = [a_3, a_1]$, $a_5 = [a_3, a_2]$

Family relations: $[a_4, a_2] = [a_5, a_1] = a_i^p$, $i = 4, 5$

Name	Name (James)	$[a_4, a_1]$	a_1^p	a_2^p
2-11-25-11	$\Phi_{43}(222)a_0$	a_6	$a_5^{-1} a_6^{\varepsilon}$	$a_4^{-\varepsilon} a_6^{-\varepsilon}$
2-11-25-12x	$\Phi_{43}(222)a_r$ $(r \neq 0)$	a_6	$a_5^{-1} a_6^{k}$	$a_4^{-\varepsilon} a_6^{l}$

Here, for every x , $1 \leq x < p$, the pair of integers k, l is one of the solutions of the following equation: $x \equiv (k-\varepsilon)^2 - \varepsilon(l+\varepsilon)^2 \pmod{p}$.

Family 2-12-11-11

Family definitions: $a_3 = a_1^p$, $a_4 = a_3^p$, $a_5 = a_4^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = e$, $3 \leq i \leq 5$

Name	Name (James)	a_5^p	$[a_2, a_1]$	a_2^p
2-12-11-11-11	(51)	a_6	.	.
2-12-11-11-12	$\Phi_2(51)$	a_6	a_6	.

Family 2-21-11

Family definitions: $a_3 = a_1^p$, $a_4 = a_2^p$, $a_5 = a_3^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = e$, $3 \leq i \leq 5$

Name	Name (James)	a_5^p	a_4^p	$[a_2, a_1]$
2-21-11-11	(42)	a_6	.	.
2-21-11-12	$\Phi_2(42)a_1$	a_6	.	a_6

Family 2-21-12

Family definitions: $a_3 = a_1^p$, $a_4 = a_2^p$, $a_5 = a_4^p$

Family relations: $[a_5, a_1] = [a_5, a_2] = [a_4, a_2] = [a_3, a_1] = e$,

$$[a_3, a_2]^{-1} = [a_4, a_1] = a_5^p$$

Name	Name (James)	a_5^p	a_3^p	$[a_2, a_1]$
2-21-12-11]	$\Phi_{14}(42)$	a_6	.	a_5

Family 2-21

Family definitions: $a_3 = a_1^p$, $a_4 = a_2^p$

Family relations: $[a_i, a_1] = [a_i, a_2]$, $i = 3, 4$

Name	Name (James)	a_3^p	a_4^p	$[a_2, a_1]$
2-21-21	(33)	a_5	a_6	.
2-21-22	$\Phi_2(33)a$	a_5	a_6	a_6

Family 2-22-11

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$, $a_5 = [a_3, a_1]$

Family relations: $[a_4, a_1] = [a_4, a_2] = [a_5, a_2] = a_3^p = a_5^p = e$

Name	Name (James)	$[a_5, a_1]$	$[a_3, a_2]$	a_4^p	a_1^p
2-22-11-11	$\Phi_9(21^4)e$	a_6	.	.	.
2-22-11-12b	$\Phi_9(21^4)b_r$	a_6	.	a_6^b	.
2-22-11-13	$\Phi_{10}(21^4)e$	a_6	a_6	.	.
2-22-11-14b	$\Phi_{10}(3111)b_r$	a_6	a_6	a_6^b	.
2-22-11-15c	$\Phi_{10}(2211)a_r$	a_6	a_6^c	.	a_6
2-22-11-16	$\Phi_9(2211)a$	a_6	.	.	a_6

Family 2-22-14

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$, $a_5 = [a_3, a_2]$

Family relations: $[a_5, a_1] = [a_4, a_1] = [a_4, a_2] = a_5^p = a_3^p = e$

Name	Name (James)	$[a_5, a_2]$	$[a_3, a_1]$	a_4^p	a_1^p
2-22-14-11	$\Phi_9(21^4)d$	a_6	.	.	.
2-22-14-12	$\Phi_{10}(21^4)d$	a_6	a_6	.	.
2-22-14-13c	$\Phi_{10}(3111)a_r$	a_6	a_6^c	a_6	.
2-22-14-14	$\Phi_9(3111)a$	a_6	.	a_6	.
2-22-14-15b	$\Phi_{10}(2211)b_r$	a_6	a_6	.	a_6^b

Family 2-22-16a

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$, $a_5 = [a_3, a_2]$

Family relations: $a_3^p = [a_4, a_1] = [a_5, a_2]^{-1}$

The range of z is $(p-3)/2 \leq z \leq 1$.

Name	Name (James)	$[a_5, a_2]$	$[a_3, a_1]$	a_4^p	a_1^p
2-22-16a-11	$\Phi_{25+x}(222)$	a_6	.	.	a_5
2-22-16a-12z		a_6	.	.	$a_5 a_6^z$
2-22-16a-13		a_6	.	.	$a_5 a_6^{-1}$
2-22-16a-14	$\Phi_{28+x}(222)$	a_6	a_6	.	a_5
2-22-16a-15	$\Phi_{25+x}(321)$	a_6	.	a_6	a_5
2-22-16a-16x	$\Phi_{28+x}(321)a_r$	a_6	a_6	a_6^x	a_5

Family 2-22-17

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$, $a_5 = a_4^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = a_3^p = e$, $i = 4, 5$

Name	Name (James)	a_5^p	$[a_3, a_1]$	$[a_3, a_2]$	a_1^p
2-22-17-11	$\Phi_2(411)c$	a_6	.	.	.
2-22-17-12a	$\Phi_3(411)b_r$	a_6	a_6^a	.	.
2-22-17-13	$\Phi_3(411)a$	a_6	.	a_6	.

Family 2-22

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$

Family relations: $[a_4, a_1] = [a_4, a_2] = a_3^p = e$

Name	Name (James)	$[a_3, a_1]$	$[a_3, a_2]$	a_4^p	a_1^p
2-22-21	$\Phi_6(21^4)d$	a_5	a_6	.	.
2-22-22a	$\Phi_6(3111)b_r$	a_5	a_6	a_5^a	.
2-22-23	$\Phi_6(2211)g$	a_5	a_6	.	a_5
2-22-24	$\Phi_6(3111)a$	a_5	a_6	a_6	.
2-22-25a	$\Phi_6(2211)h_r$	a_5	a_6	.	a_6^a
2-22-26a	$\Phi_6(321)b_{r,1}$	a_5	a_6	a_5^a	a_6
2-22-27a	$\Phi_6(321)b_{r,\gamma}$	a_5	a_6	a_5^a	a_6^ε
2-22-28x	$\Phi_6(321)a_r$	a_5	a_6	a_6	a_5^x

Family 2-23-12

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$, $a_5 = a_4^p$

Family relations: $[a_5, a_1] = [a_5, a_2] = [a_3, a_1] = [a_4, a_2] = [a_4, a_3] = e$

$[a_4, a_1] = [a_3, a_2]^{-1} = a_3^p$

Name	Name (James)	a_5^p	$[a_3, a_2]$	a_1^p
2-23-12-11	$\Phi_2(42)a_2$	a_6	.	a_3
2-23-12-12]	$\Phi_8(42)$	a_6	a_6	a_3

Family 2-23

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$

Family relations: $[a_4, a_2] = [a_3, a_1] = e$, $[a_4, a_1] = [a_3, a_2]^{-1} = a_3^p$

Name	Name (James)	$[a_3, a_2]$	a_4^p	a_1^p
2-23-21	$\Phi_8(33)$	a_5	a_6	a_3

Famil 2-31

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_1^p$, $a_5 = a_2^p$

Family relations: $[a_4, a_1] = [a_5, a_1] = e$, $[a_4, a_2]^{-1} = [a_5, a_1] = a_3^p$

Name	Name (James)	$[a_3, a_1]$	$[a_3, a_2]$	$[a_4, a_2]$	a_4^p	a_5^p
2-31-11	$\Phi_3(3211)g$	a_6	.	.	.	.
2-31-12	$\Phi_8(321)c_{p-1}$	a_6	.	a_6	.	.
2-31-13α	$\Phi_3(321)c_r$	a_6	.	.	.	a_6^α
2-31-14x	$\Phi_8(321)c_r$	a_6	.	a_6	.	a_6^x
2-31-15	$\Phi_3(321)a$	a_6	.	.	a_6	.
2-31-16	$\Phi_8(222)$	a_6	.	a_6	a_6	.
2-31-17	$\Phi_2(321)f$	.	.	.	a_6	.
2-31-18	$\Phi_{14}(222)$	.	.	a_6	.	.
2-31-19	$\Phi_{14}(321)$	.	.	a_6	a_6	.

SOME GROUPS OF ORDER p^7, p^8

Family 2-12-11-11-11

Family definitions: $a_3 = a_1^p$, $a_4 = a_3^p$, $a_5 = a_4^p$, $a_6 = a_5^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = e$, $3 \le i \le 6$

Name	a_6^p	$[a_2, a_1]$	a_2^p
2-12-11-11-11-11	a_7	.	.
2-12-11-11-11-12]	a_7	a_7	.

Family 2-21-11-11

Family definitions: $a_3 = a_1^p$, $a_4 = a_2^p$, $a_5 = a_3^p$, $a_6 = a_5^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = e$, $3 \le i \le 6$

Name	a_6^p	a_4^p	$[a_2, a_1]$
2-21-11-11-11	a_7	.	.
2-21-11-11-12	a_7	.	a_7

Family 2-21-11-12

Family definitions: $a_3 = a_1^p$, $a_4 = a_2^p$, $a_5 = a_3^p$, $a_6 = a_5^p$

Family relations: $[a_3, a_1]^{-1} = [a_4, a_1] = a_6^p$

Name	a_6^p	a_4^p	$[a_2, a_1]$
2-21-11-12-11]	a_7	.	a_6

Family 2-21-21

Family definitions: $a_3 = a_1^p$, $a_4 = a_2^p$, $a_5 = a_3^p$, $a_6 = a_4^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = e$, $3 \le i \le 6$

Family 2-21-21 (continued)

Name	a_5^p	a_6^p	$[a_2, a_1]$
2-21-21-11	a_7	.	.
2-21-21-12	a_7	.	a_7
2-21-21-21	a_7	a_8	.
2-21-21-21	a_7	a_8	a_8

Family 2-22

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = a_3^p = e$, $i = 4, 5$

Name	$[a_3, a_1]$	$[a_3, a_2]$	a_4^p	a_1^p
2-22-31	a_5	a_6	a_7	.
2-22-32a	a_5	a_6	a_7	a_6^a
2-22-33	a_5	a_6	a_7	a_5

Family 2-23-12-11

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$, $a_5 = a_4^p$, $a_6 = a_5^p$

Family relations: $[a_i, a_1] = [a_i, a_2] = [a_4, a_2] = [a_3, a_1] = e$,

$i = 5, 6$, $[a_4, a_1]^{-1} = [a_3, a_2] = a_3^{-p}$

Name	a_6^p	$[a_4, a_1]$	a_1^p
2-23-12-11-11	a_7	.	a_3
2-23-12-11-12	a_7	a_7	a_3

Family 2-23-21

Family definitions: $a_3 = [a_2, a_1]$, $a_4 = a_2^p$, $a_5 = a_3^p$, $a_6 = a_4^p$

Family relations: $[a_6, a_2] = [a_5, a_1] = [a_4, a_2] = [a_3, a_1] = e$,

$$[a_5, a_2] = [a_6, a_1] = [a_4, a_3] = a_5^{-p} ,$$

$$[a_4, a_1] = a_5^{p-1} = [a_5, a_2]^{-(p-3)/2} , \quad a_3^p = a_5^{-1}$$

Name	a_5^p	a_6^p	a_1^p
2-23-21-11	a_7	.	a_3
2-23-21-12	.	a_7	a_3
2-23-21-21	a_7	a_8	a_3

REFERENCES

Ascione, J. [1979]: On 3-groups of second maximal class (PhD thesis, Australian National University, Canberra).

Ascione, J., Havas, G., Leedham-Green, C.R. [1977]: A computer aided classification of certain groups of prime power order, *Bull. Austral. Math. Soc.* **17**, 257-275.

Ascione, J., Havas, G., Leedham-Green, C.R. [1977]: A computer aided classification of certain groups of prime power order: Corrigendum and Microfiche supplement, *Bull. Austral. Math. Soc.* **17**, 317-320.

Bagnera, G. [1898]: La composizione dei gruppi finiti il cui grado è la quinta potenza di un numero primo, *Ann. Mat. Pura Appl.* (3) **1**, 137-338.

Bagnera, G. [1899]: Sopra i gruppi di grado 32 , *Ann. Mat. Pura Appl.* (3) **2**, 263-275.

Bender, H.A. [1927]: A determination of the groups of order p^5 , *Ann. of Math.* (2) **29**, 61-72.

Hall, M. and Senior, J.K. [1964]: *The Groups of Order* 2^n $(n \leq 6)$. (Macmillan, New York).

Hall, P. [1940]: The classification of prime-power groups, *J. Reine Angew. Math.* **182**, 130-141.

Havas, G. and Nicholson, T. [1976]: Collection. *SYMSAC '76*, 9-14 (Proc. ACM Sympos. Symbolic and Algebraic Computation, New York, 1976. Association for Computing Machinery, New York).

Higman, G. [1960]: Enumerating p-groups I: Inequalities, *Proc. London Math. Soc.* **10**, 24-30.

Higman, G. [1960]: Enumerating p-groups II: Problems whose solution is PORC, *Proc. London Math. Soc.* **10**, 566-582.

Hölder, O. [1893]: Die Gruppen der Ordnung p^3, pq^2, pqr, p^4 , *Math. Ann.* **43**, 301-412.

Huppert, B. [1967]: *Endliche Gruppen I* (Springer-Verlag, Berlin, Heidelberg, New York).

James, R.K. [1969]: The groups of order p^6 $(p \geq 3)$ (PhD thesis, University of Sydney, Sydney).

James, R.K. [unpublished]: The groups of order p^6 $(p \geq 3)$. Corrected List.

Miller, G.A. [1899]: Report on recent progress in the theory of the groups of a finite order, *Bull. Amer. Math. Soc.* 5, 227-249.

Netto, E. [1882]: *Substitutionen theorie und ihre Anwendungen auf die Algebra* (Teubner, Leipzig).

Newman, M.F. [1977]: Determination of groups of prime-power order. *Group Theory*, Canberra 1975, 73-84 (Proc. Miniconf. Australian National University, 1975. Lecture Notes in Mathematics, 573. Springer-Verlag, Berlin, Heidelberg, New York).

Newman, M.F. [1976]: Calculating presentations for certain kinds of quotient groups. *SYMSAC '76*, 2-8 (Proc. ACM Sympos. Symbolic and Algebraic Computation, New York, 1976. Association for Computing Machinery, New York).

Rotman, J.J. [1965]: *The Theory of Groups* (Allyn Bacon, Boston).

Wamsley, J.W. [1974]: Computation in nilpotent groups (theory). *Proc. Second Internat. Conf. Theory of Groups*, Canberra, 1973, 691-700 (Lecture Notes in Mathematics, 372. Springer-Verlag, Berlin, Heidelberg, New York).

Young, J.W.A. [1893]: On the determination of groups whose order is a power of a prime, *Amer. J. Math.* 15, 124-178.